FREEDOM OF INFORMATION
AND PROTECTION OF PRIVACY

Freedom of Information and Protection of Privacy

GUIDELINES AND PRACTICES

September 2000

Alberta
GOVERNMENT OF ALBERTA

Produced by

Information Management and Privacy
Alberta Municipal Affairs
201, 10808 - 99 Avenue
Edmonton, Alberta, Canada
T5K 0G5

Phone: (780) 422-2657
Fax: (780) 427-1120
Web site: http://www.gov.ab.ca/foip

©Government of Alberta

ISBN 077851000X

INTRODUCTION

This publication provides a comprehensive reference tool for the application of the *Freedom of Information and Protection of Privacy (FOIP) Act* by all organizations that are subject to the *Act* in Alberta. It interprets the *Act* and the FOIP Regulation, sets out roles and responsibilities, and offers guidance on approaches and procedures. It is intended to be used by staff who will be processing FOIP requests and carrying out privacy protection measures.

This publication is provided as information only, and is intended to serve as a supplement to the *FOIP Act* and Regulation. The information contained in it is provided as a guideline, not as binding rules, except for a limited number of policy statements that are clearly indicated in **bold text**.

All examples used are provided as illustrations and should not be used as authority for any decisions made under the *Act*. This publication is not to be used as a substitute for legal advice. In case of any doubt as to the proper application of the *Act*, please refer to the FOIP Coordinator of your public body.

This edition of *Freedom of Information and Protection of Privacy: Guidelines and Practices* incorporates amendments to the FOIP legislation up to July 1, 2000, including the amendments introduced in the *Freedom of Information and Protection of Privacy Amendment Act, 1999*. References to the *FOIP Act* and the FOIP Regulation appear in bold text. References to other legislation are in plain text.

The Office of the Information and Privacy Commissioner publishes Orders, Practice Notes and Investigation Reports. Alberta Municipal Affairs, Information Management and Privacy, publishes FOIP Bulletins and other guidelines. This publication references policy and guideline information, and Commissioner's Orders released up to July 1, 2000.

For further information about the administration or operation of the *Act*, please contact:

Information Management and Privacy
Alberta Municipal Affairs
201, 10808 - 99 Avenue *
Edmonton, Alberta T5K 0G5 *
Phone: (780) 422-2657
Fax: (780) 427-1120
Web site: http://www.gov.ab.ca/foip

* Effective October 2000, our mailing address will be 16th Floor, Commerce Place, 10155 - 102 Street, Edmonton, T5J 4L4.

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

Guidelines and Practices

Table of Contents

Chapter 1: Overview **1**

1.1 Purposes of *FOIP Act* 1
1.2 Public Bodies Within the Scope of the *Act* 1
1.3 Organizations Not Within the Scope of the *Act* 3
1.4 Scope of the *Act* 4
1.5 Records Covered by the *Act* 5
1.6 Custody or Control 6
1.7 Records Excluded from the *Act* 7
1.8 Accessing Information 14
1.9 Routine Access to Information 15
1.10 Practices for Routine Disclosure and Active Dissemination 18

Chapter 2: Administration of the *FOIP Act* **23**

2.1 Public Body - Roles and Responsibilities 23
2.2 Delegation of FOIP Responsibilities 26
2.3 Province-Wide Administration of the *Act* 27
2.4 Liability, Sanctions and Penalties 29

Chapter 3: Access to Records **31**

3.1 Who Has a Right of Access 31
3.2 Access Tools 31
3.3 Receiving a FOIP Request 33
3.4 Processing a FOIP Request 46
3.5 Responding to a FOIP Request 62

Chapter 4: Exceptions to the Right of Access 67

4.1 Overview 67
4.2 Relationship to Other Acts 72
4.3 Disclosure Harmful to Business Interests of a Third Party.... 73
4.4 Disclosure Harmful to Personal Privacy 82
4.5 Disclosure Harmful to Public or Individual Safety 98
4.6 Confidential Evaluations 102
4.7 Disclosure Harmful to Law Enforcement 105
4.8 Intergovernmental Relations 119
4.9 Cabinet and Treasury Board Confidences 124
4.10 Local Public Body Confidences 130
4.11 Advice from Officials 135
4.12 Economic and Other Interests of a Public Body or the Government of Alberta 145
4.13 Testing Procedures 152
4.14 Privileged Information 153
4.15 Disclosure Harmful to Historical Resources, Rare, Endangered or Vulnerable Life 164
4.16 Information That Is or Will Be Published 165

Chapter 5: Third Party Intervention and Notice 167

5.1 Overview 167
5.2 When is Third Party Notification Required? 167
5.3 How is a Third Party Notification Process Carried Out? 168
5.4 Content of Third Party Notice 169
5.5 Notice to Applicant 170
5.6 Response from Third Party 170
5.7 Notice of Decision 171
5.8 Time Limits 172
5.9 Time Extension 174

Chapter 6: Disclosure in the Public Interest 179

6.1 Overview 179
6.2 Disclosure 179
6.3 Public Interest 181
6.4 Determination of Public Interest 182
6.5 Scope 183
6.6 Notification 183
6.7 Review 184
6.8 Disclosure to the Commissioner 184

Chapter 7: Protection of Privacy........**187**

7.1 Overview........187
7.2 Purposes of Collection........189
7.3 Manner of Collection........192
7.4 Accuracy and Retention........201
7.5 Correction of Personal Information........203
7.6 Protection of Personal Information........208
7.7 Use of Personal Information........211
7.8 Disclosure of Personal Information........215
7.9 Consistent Uses........237
7.10 Disclosure for Research or Statistical Purposes........238
7.11 Disclosure of Information in Archives........242
7.12 Record of Purposes........245
7.13 Exercise of Individual Rights by Other Persons........246

Chapter 8: Records and Information Management........**249**

8.1 Overview........249
8.2 Scope........249
8.3 Powers of the Commissioner........250
8.4 Records Issues Relating to Access Requests........250
8.5 Records and Information Management Principles........253
8.6 Records and Information Management Policy Components........254

Chapter 9: Privacy and Information Management........**261**

9.1 Overview........261
9.2 Privacy and Security Impact Assessments........263
9.3 Checklist for the Review of Personal Information Systems........266
9.4 Review of Forms........274
9.5 Security Policy and Practices........277
9.6 Data Sharing and Data Matching........281

Chapter 10: Information and Privacy Commissioner........**287**

10.1 Overview........287
10.2 Appointment........287
10.3 Mandate and Powers........287
10.4 Monitoring Role........289
10.5 Provision of Advice........290

10.6 Disclosure to the Commissioner 291
10.7 Powers 291
10.8 Access to Information 291
10.9 Power to Disregard Requests 292
10.10 Statements Provided to the Commissioner 294
10.11 Protection from Liability 294
10.12 Delegation of the Commissioner's Powers 295
10.13 Reviews and Investigations 295
10.14 Adjudicator Process 302
10.15 Judicial Review 303

APPENDIXES:

Appendix 1: Definitions 305

Appendix 2: Delegation Table 317

Appendix 3: Model Letters 323

Appendix 4: Privacy Reviews and Compliance Audits 369

Appendix 5: Model FOIP Request Charts 379

Appendix 6: *Freedom of Information and Protection of Privacy Act* Forms 389

INDEXES:

Index of *Freedom of Information and Protection of Privacy Act* and Regulation Citations 393

Index of Information and Privacy Commissioner's Order and Investigation Report Citations 403

Index of Words and Phrases Discussed or Defined 407

Subject Index 415

Chapter 1
Overview

1.1 PURPOSES OF THE *FOIP ACT*

The basic objectives of the *FOIP Act* are to ensure that public bodies are open and accountable to the public by providing a right of access to records and by protecting the personal privacy of individuals.

Section 2 of the *Act* sets out five purposes.

***A right of access to records*:** The first purpose is to establish a right of access by any person to records in the custody or under the control of a public body, subject to limited and specific exceptions which are set out in the *Act*.

This right of access is the cornerstone of openness and accountability of public bodies and should be taken into account when making any decision about disclosing records in response to a FOIP request.

The limited and specific exclusions and exceptions which are set out in the *Act* provide the only basis for refusing access to records and should always be interpreted with a view to giving as much access as possible to the records requested.

***Protection of personal privacy*:** The second purpose is to control the manner in which a public body may collect personal information from individuals, the use that it may make of that information, and its disclosure of that information.

***A right of access to an individual's own personal information*:** The third purpose is to create a right of access for individuals to personal information about themselves, again subject to limited and specific exceptions set out in the *Act*.

The exceptions should always be interpreted with a view to giving an individual as much access as possible to his or her own personal information.

***A right of correction*:** The fourth purpose is to allow individuals a right to request corrections to personal information about themselves that is held by a public body.

***Independent review of decisions*:** The fifth purpose is to provide for the independent review of decisions made by public bodies under the *Act* and for the investigation of complaints. Independent review is provided by the Information and Privacy Commissioner.

1.2 PUBLIC BODIES WITHIN THE SCOPE OF THE ACT

The *FOIP Act* applies to public bodies. A *public body* is defined in **section 1(1)(p)** of the *Act* as:

- a department, branch or office of the Government of Alberta;
- an agency, board, commission, corporation, office, or other body listed in **Schedule 1** of the FOIP Regulation;

- the Executive Council Office;
- the office of a member of the Executive Council;
- the Legislative Assembly Office;
- the offices of the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner, and the Information and Privacy Commissioner; or
- a local public body.

Public bodies, other than local public bodies, are referred to collectively in this publication as **provincial public bodies**.

Section 1(1)(j) defines a *local public body* as:

- an educational body;
- a health care body; or
- a local government body.

Educational body **(section 1(1)(d)):** An educational body is defined in the *Act* to mean:

- a university as defined in the *Universities Act*;
- a technical institute as defined in the *Technical Institutes Act*;
- a public college as defined in the *Colleges Act*;
- the Banff Centre as defined in the *Banff Centre Act*;
- a board as defined in the *School Act;*
- a charter school as defined in the *School Act*; or
- a Regional authority as defined in the *School Act*.

Health care body **(section 1(1)(g)):** A health care body is defined in the *Act* to mean:

- the board of an approved hospital as defined in the *Hospitals Act*, other than an approved hospital that is owned and operated by a regional health authority under the *Regional Health Authorities Act;*
- the operator of a nursing home as defined in the *Nursing Homes Act*, other than a nursing home owned and operated by a regional health authority under the *Regional Health Authorities Act;*
- a provincial health board established under the *Regional Health Authorities Act*;
- the Alberta Cancer Board;
- a regional health authority under the *Regional Health Authorities Act*;
- a community health council established under the *Regional Health Authorities Act*; or
- a subsidiary health corporation as defined in the *Regional Health Authorities Act*.

Hospitals and nursing homes directly owned and operated by a regional health authority are part of the regional health authority. Other public hospitals and nursing homes are separate local public bodies.

Local government body **(section 1(1)(i)):** A local government body is defined in the *Act* to mean:

- a municipality as defined in the *Municipal Government Act;*
- an improvement district under the *Municipal Government Act;*
- a special area as defined by the *Special Areas Act*;
- a regional services commission under **Part 15.1** of the *Municipal Government Act;*

- a board established under the *Drainage Districts Act*;
- a board established under the *Irrigation Act*;
- a management body established under the *Alberta Housing Act*, a housing authority continued under **section 37** of the *Alberta Housing Act* or a foundation continued as a management body under **section 38** of that *Act*;
- a Metis settlement established under the *Metis Settlements Act*;
- the Metis Settlements General Council established under the *Metis Settlements Act*;
- any commission, police service or policing committee as defined in the *Police Act;*
- any municipal library board, library system boards, federation board or joint municipal library board established or continued under the *Libraries Act*; or
- any board, committee, commission, panel, agency or corporation that is created or owned by any of the bodies listed above and where all the members or officers of which are appointed or chosen by that body.

Police services and police commissions are separate public bodies.

1.3 ORGANIZATIONS NOT WITHIN THE SCOPE OF THE *ACT*

Section 1(1)(p) specifically excludes the following from the *Act*:

- the office of the Speaker of the Legislative Assembly;
- the office of a Member of the Legislative Assembly; and
- the Court of Appeal of Alberta, the Court of Queen's Bench of Alberta, the Surrogate Court of Alberta and the Provincial Court of Alberta.

Since government departments are public bodies and the Executive Council Office is a public body, but the office of a Member of the Legislative Assembly is not, some records of Members of the Executive Council (Cabinet members) will fall within the scope of the *Act* and others will not. The records of Members of the Executive Council that relate to their duties in Cabinet and in the administration and operation of a public body are within the scope of the *Act*, but records that relate to their duties as MLAs are not.

Section 1(1)(i) defines local government body to exclude certain agencies from the *Act*.

EPCOR Utilities Inc. and ENMAX Corporation and any of their subsidiaries that own a gas utility, a generating unit, transmission facility or electric distribution system, or whose primary business activity is providing electricity services are excluded.

As well, community library boards established under the *Libraries Act* are not public bodies under the *Act*. However, if a community library board receives assistance from a municipality or a government department, records relating to that assistance may be available from the municipality or government department.

The RCMP and First Nations Police Services are not public bodies under the *FOIP Act*.

Section 1(1) of the *Act* is concerned in a number of definitions with establishing which *organizations* are and are not public bodies for the purposes of the *Act*, that is to say, which organizations are subject to the *Act* and therefore have statutory duties with regard to access to information and protection of privacy.

Section 4 of the *Act* is concerned with defining which *records* are subject to the *Act*. **Section 4** is discussed in section 1.7 of this chapter.

1.4 SCOPE OF THE *ACT*

The *FOIP Act* is **in addition to** and **does not replace existing procedures** for obtaining access to information or records held by public bodies. However, any routine disclosure of personal information by public bodies must be in compliance with **Part 2** of the *Act* (**section 3(a)**).

Routine disclosure of information is discussed in more detail in section 1.9 of this chapter.

The *Act* does not affect access to records in the Provincial Archives of Alberta, or any other archives of a public body, if public access to the records was not restricted before the *Act* came into force with respect to those archives (**section 3(b)**).

If an archival institution serving a public body declared a group of records open to public access before the public body became subject to the *Act*, those records remain open to public access regardless of the provisions of the FOIP legislation.

For provincial public bodies, the *Act* came into force on October 1, 1995. The *Act* came into force for local public bodies on different proclamation dates between September 1, 1998, and October 1, 1999.

The *Act* does not limit the information otherwise available by law to a party to legal proceedings (**section 3(c)**).

Legal proceedings are activities governed by rules of court or rules of judicial or quasi-judicial tribunals that can result in a judgment of a court or a ruling by a tribunal. **Section 3(c)** means that the *Act* does not prevent or limit the use of legal processes such as examination for discovery to gather information about a party in a lawsuit.

It is relatively common for persons involved in a criminal or civil legal action to make a FOIP request to a public body for records relating to the case. Such a request should be processed as a FOIP request, applying the provisions of the *Act*.

If an action proceeds to discovery, or if some other legal procedure is invoked to obtain disclosure of records, the rules governing that legal procedure will apply. The access provisions of the *FOIP Act* are applicable only to requests made under the *FOIP Act* and not to other legal processes. It is common to have both processes going on at the same time. See, for example, the discussion in *IPC Order 97-009*.

The provisions of the *Act* do not override the power of any court or tribunal to compel a witness to testify or to compel the production of documents (**section 3(d)**).

The *Act* does not prohibit the transfer, storage or destruction of a record in accordance with an enactment of Alberta or Canada, or, in the case of local public bodies, sanctioned by by-law, resolution or other legal instrument by which a local public body acts (**section 3(e)**).

This permits the orderly disposition of records by public bodies in accordance with records retention and disposition schedules.

If a local public body has no by-law, resolution or other legal instrument with respect to the transfer, storage or destruction of records, it may carry out these functions in accordance with a policy authorized by the governing body of the local public body.

See Chapter 8 of this publication for more on records and information management, including the effect of **section 34(b)** of the *Act* on the disposition of records.

1.5 RECORDS COVERED BY THE *ACT*

The *Act* applies to all the records *in the custody* or *under the control* of a public body, including court administration records (**section 4(1)**).

Definition of Record

Record means recorded information in any form, including books, documents, maps, drawings, photographs, letters, vouchers, papers, and any other information that is written, photographed, recorded or stored in any manner (**section 1(1)(q)**).

Any recorded information, including handwritten notes and electronic correspondence or messages, which is in the custody or control of a public body is a record for the purposes of the *Act*.

However, software and other mechanisms used to produce records are not considered records for purposes of the legislation.

Definition of Personal Information

The *Act* defines *personal information* as recorded information about an identifiable individual, including, but not limited to:

- the individual's name, home or business address or home or business telephone number;
- the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;
- the individual's age, sex, marital status or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, blood type or inheritable characteristics;
- information about the individual's health and health care history, including information about a physical or mental disability;
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- anyone else's opinions about the individual; and

- the individual's personal views or opinions, except if they are about someone else (**section 1(1)(n)**).

1.6 CUSTODY OR CONTROL

A public body has *custody* of a record when the record is in the possession of the public body (see *IPC Order 2000-005*).

A record is under the *control* of a public body when the public body has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition.

Some indicators that a record may be in the custody or under the control of a public body are as follows:

- the record was created by an officer, employee or member of the public body;
- the record was created by an outside contracted consultant for the public body;
- the record is specified in a contract as being under the control of a public body;
- the record is in the possession of the public body;
- the record is closely integrated with other records of the public body;
- the content of the record relates to the public body's mandate and functions;
- the public body has the authority to regulate the record's use and disposition;
- the public body has relied upon the record to a substantial extent; or
- a contract permits the public body to inspect, review or copy records produced, received or acquired by a contractor as a result of a contract.

(See IPC Order 99-032.)

The most common situation where a public body may have control, but not custody, of a record is in the case of contracted services. The record is created by and in the possession of the contractor, but the public body has set out some rights of access in the contract.

For example, general clauses such as the following are often found in contracts:

- The contractor will keep and make available to the public body, upon request, records in a form that will allow the public body to determine that the services are being provided, upon the request of the public body.

- The contractor will furnish such information and particulars, as required by the public body, concerning the services and the care and progress of persons receiving services, upon the request of the public body.

In such cases, records used by the public body to monitor or inspect the delivery of the services would be deemed to be under its control.

If a counsellor under contract to a public body maintains notes of his or her counselling activities on behalf of the public body in his or her office or home, such notes are likely to be considered to be under the control of the public body for purposes of the *FOIP Act*.

Administrative records relating to the business of a contractor would not normally be considered to be under the control of a public body unless this was specifically stipulated in the contract. If a contractor deals with a subcontractor, but a public body does not exercise any rights in regard to the records relating to the work of the subcontractor, those records will not be under the control of a public body.

A fuller discussion of FOIP and contract management is found in the publication *Freedom of Information and Protection of Privacy: Contract Manager's Guide*, produced by Information Management and Privacy, Alberta Municipal Affairs.

All public bodies should review their contracting practices to ensure that they adequately take the *FOIP Act* into account.

There may be situations, such as a records storage centre, where both control and custody lie with the public body storing the records and not with the organization offering the storage service.

1.7 RECORDS EXCLUDED FROM THE *ACT*

A limited number of records in the custody or under the control of public bodies are excluded from the application of the *Act*. These are as follows.

***Certain categories of court and judicial records* (section 4(1)(a)):** Information in a court file, a record of a judge of the Court of Appeal of Alberta, the Court of Queen's Bench of Alberta, or The Provincial Court of Alberta, a record of a master of the Court of Queen's Bench of Alberta, a record of a sitting or presiding justice of the peace, or a judicial administration record or a record relating to support services provided to the judges of any of the courts referred to above is not within the scope of the *Act*.

The term *judicial administration record* is defined in **section 4(2)** of the *Act* and in the **Definitions** in Appendix 1 of this publication.

***Draft judicial or quasi-judicial decisions* (section 4(1)(b)):** A personal note, communication or draft decision created by or for a person who is acting in a judicial or quasi-judicial capacity is not within the scope of the *Act*. This includes any authority designated by the Lieutenant Governor in Council that is subject to the *Administrative Procedures Act*.

This exclusion also applies to communications between the members of the judicial or quasi-judicial body themselves, and between members and support staff, when these communications relate to the judicial or quasi-judicial functions of the body.

The exclusion does not apply to decisions or reasons of the judicial or quasi-judicial body, although another exclusion or exception may apply to these records.

A *personal note* of a member of a judicial or quasi-judicial tribunal is one intended solely for the use of the person who wrote it (see *IPC Order 99-025*).

The following criteria, which are not exhaustive, should be reviewed in determining whether a body is acting in a "judicial or quasi-judicial capacity":

- Is there anything in the language in which the function is conferred or in the general context in which it is exercised which suggests that a hearing is contemplated before a decision is reached?
- Does the decision or order directly or indirectly affect the rights and obligations of persons?
- Is the adversarial process involved?
- Is there an obligation to apply substantive rules to many individual cases rather than, for example, the obligation to implement social and economic policy in a broad sense?

(See *IPC Order 99-025.*)

No one factor is decisive and it will be necessary to consider the legislation under which a decision is made to see whether the rules of natural justice apply. The nature of the issue to be decided and the importance of the decision for those affected should also be examined. Public bodies may wish to seek legal advice when dealing with these issues.

Examples of provincial public bodies that make quasi-judicial decisions are the Alberta Energy and Utilities Board, the Environmental Appeal Board and the Board of Reference. Examples at the local government level are the Subdivision and Development Appeal Board and the Assessment Review Board. Such bodies make rulings of a judicial, as opposed to an administrative, nature.

***Quality assurance records of health care bodies* (section 4(1)(b.1)):** Quality assurance committees study, assess and evaluate the provision of health services with a view to continuous improvement. Under section 9 of the *Alberta Evidence Act*, certain records of, and documentation supplied to, quality assurance committees in health care bodies are not admissible as evidence in court. The *FOIP Act* does not apply to these quality assurance records.

This exclusion applies *only* to the records of quality assurance committees as defined in the *Alberta Evidence Act* and not to other quality assurance committees established within health care bodies and other public bodies to monitor the quality of health services or other services.

The exclusion for the records of quality assurance committees does not extend to original medical and hospital records of a patient even if they were supplied to a quality assurance committee.

***Records of an Officer of the Legislature* (section 4(1)(c)):** A record that is created by or for or is in the custody or under the control of an Officer of the Legislature, and relates to the exercise of that officer's functions under an Act of Alberta, is not within the scope of the *Act*.

Operational files and correspondence of the Auditor General, the Information and Privacy Commissioner, the Ethics Commissioner, the Chief Electoral Officer, and the Ombudsman are excluded from the coverage of the *Act*. Correspondence to and from these offices is excluded regardless of where the files or correspondence are located. This includes letters and draft reports in the custody of a public body. It also includes records created by employees and contractors for these officers. (See *IPC Order 97-008.*)

The administrative files of these legislative offices, however, are subject to the *Act*. These include personnel information, contracts and general office management records.

***Records of the Ethics Commissioner* (section 4(1)(c.1) and (c.2)):** There are two parts to this exclusion.

First, information is excluded if it is collected by or for or is in the custody or under the control of the Ethics Commissioner, and relates to the disclosure statements of deputy ministers and other senior officers that have been deposited with the Ethics Commissioner. This provision covers records created from information provided to the Ethics Commissioner.

Second, records are excluded if they are created by or for or are in the custody or under the control of the Ethics Commissioner relating to any advice about conflicts of interest, whether or not the advice was given under the *Conflicts of Interests Act*.

***A question to be used on an examination or test* (section 4(1)(d)):** A question to be used on an examination or test is not within the scope of the *Act*. This exclusion applies to questions that are to be used in the future. It includes question banks from which questions are to be selected for future tests. The exclusion does not apply to test banks containing tests administered in the past which might be used as a source of future questions for tests.

Questions that were used in previous tests, but which will not be used again, are subject to the *Act*.

***Teaching and research materials* (section 4(1)(e) and (e.1)):** The *Act* does not apply to teaching materials of employees of a post-secondary educational body or of the post-secondary educational body itself. Nor does it apply to teaching materials of both employees and the post-secondary educational body.

This provision is intended to ensure that the access provisions of the *Act* do not compromise the intellectual property rights – including the right to priority of publication – of those responsible for the creation of post-secondary teaching materials and research information. *Teaching materials* include records produced or compiled for the purpose of providing systematic instruction to a person about a subject or skill and include records created or compiled to aid the instructor in imparting information, or for distribution to students.

Also excluded from the scope of the *FOIP Act* is research information of employees of a post-secondary educational body.

Research information includes records produced or compiled as part of a research project, and include data, working papers, bibliographies and other materials used in the research process.

This exclusion is limited and does not extend to all research materials used in a university, college, technical institute, or the Banff Centre.

Post-secondary educational body means one of the educational bodies defined in the *FOIP Act*, but not one that is defined in the *School Act*.

***Archival materials* (section 4(1)(f)):** Material that has been deposited in the Provincial Archives of Alberta or in the archives of a public body by or for a person or entity other than a public body is not within the scope of the *Act*.

Individuals, corporations, labour unions, churches, and other groups may place collections of papers in the archives of public bodies. These materials may continue to be owned by the depositing body or may be given to the archives. These records are not subject to the *Act*.

This provision also applies to records of Members of the Executive Council who held office prior to April 1, 1995, if the records relate to a term of office prior to that date and were donated to the Provincial Archives of Alberta. These records are considered to be private records. Records relating to a term of office after that date are subject to the *Act*.

***Records relating to an ongoing prosecution* (section 4(1)(g)):** The *Act* does not apply to a record relating to a prosecution, if all proceedings in respect of the prosecution have not been completed.

Prosecution records are excluded until the appeal period has expired and, in a case where Crown counsel has stayed a criminal prosecution, until the one-year period from the stay has expired.

The exclusion here is to permit a legal proceeding to take place uninhibited by FOIP requests. However, before the proceeding takes place, and after any stay or appeal period has expired, the *FOIP Act* applies to the records involved. See also Chapter 4.7 of this publication for records relating to the exercise of prosecutorial discretion.

***Public registries* (section 4 (1)(h)):** The *Act* does not apply to a record made from information in:

- the Personal Property Registry;
- the office of the Registrar of Motor Vehicle Services;
- the office of the Registrar of Corporations;
- the office of the Registrar of Companies;
- a Land Titles Office;
- an office of a district registrar as defined in the *Vital Statistics Act*; or
- a registry operated by a public body where public access is normally permitted.

This provision recognizes that there are a number of public registries that record information for particular purposes and have been recognized as important to the functioning of a variety of social, economic and regulatory activities. These include licensing of drivers, transfer of land, corporate ownership and the securing of debt.

Most public registries contain personal information that would otherwise be protected from disclosure. However, the disclosure of this information, and procedures for obtaining access to the information, are already regulated by law.

The exclusion applies to any record made from such a registry, whether in the custody of the public body operating the registry or of another public body. The exclusion applies only to the records. The *Act* still applies to the collection of the information (see *IPC Investigation Report 99-001*).

Records of elected officials of local public bodies **(section 4 (1)(i)):** A personal or constituency record of an elected official of a local public body, such as a school trustee or municipal councillor, is excluded from the coverage of the *Act* (see *IPC Order 99-032*).

The onus will be on the elected official to show that the records are not related in any way to the business of the municipality, school board, Metis settlement, or other local public body to which the official has been elected.

Constituency records relate to an elected official's constituency office, those who may have worked on an election campaign and details about the campaign.

Examples of such records include:

- private correspondence of an elected official that has not been sent or received by the official in his or her capacity as an officer of the local public body but which may be maintained in his or her public office for convenience;
- records relating to the election campaign of an elected official of a local public body, other than those records required to be submitted to the authority governing the election;
- personal notes created solely as a memory aid and not scheduled for retention by the public body;
- records of personal or family appointments or events, such as medical appointments, birthdays, vacations or financial transactions;
- records related to a community organization or non-profit group to which the individual belongs on a personal basis not as a representative of the public body; and
- records related to a commercial or private business enterprise in which the individual is employed, holds office or of which he or she is an owner, director, shareholder or partner.

The following are useful guidelines for elected officials in determining whether records are excluded from the scope of the *Act*:

- the record is not deposited with the administration of the local public body;
- the local public body has no power to compel the elected official to produce the records, even when referred to in a meeting of elected officials;
- the local public body has no authority to regulate or dispose of the records;
- the record exists and is referred to as a part of the elected official's mandate to represent the constituent, not as a basis for action by the local public body; and
- the records are not integrated with other local public body records in the office of the elected official.

For more information on this exclusion see *FOIP Bulletin No. 6, Records of*

Elected and Appointed Officials of Local Public Bodies.

***Personal records of appointed members of the governing body of a local public body* (section 4 (1)(i.1)):** Personal records of appointed members of governing bodies of local public bodies are excluded from the *Act*.

Governing body means the body that has the statutory authority to govern and make decisions affecting the local public body. This includes library boards, boards of housing management bodies and regional health authority boards.

For post-secondary educational bodies, the term is defined in **section 4(1.1)** to mean the board of governors and the general faculties council or academic council as applicable.

In addition to the relevant examples cited above with respect to elected officials (**section 4 (1)(i)**), the exclusion for personal records of appointed governing body members might cover:

- records related to a professional or similar organization to which the individual belongs or in which he or she holds office;
- biographical and historical material about the individual which has not been made public;
- records related to previous jobs or appointments of the appointee;
- references given to individuals not employed by the local public body; or
- research, speeches, lecture notes and similar items which are not related to the local public body and which were not produced at the expense of the local public body.

For more information on this exclusion see *FOIP Bulletin No. 6, Records of Elected and Appointed Officials of Local Public Bodies.*

***Personal or constituency records of a member of the Executive Council* (section 4(1)(j)):** A personal record or constituency record of a member of the Executive Council is not within the scope of the *Act*.

This means that records that relate to the duties of a member of the Executive Council as an MLA are excluded from the scope of the *Act*, but records that relate to duties in Cabinet and in the administration and operation of a public body are within the scope of the *Act*.

***Record of the Speaker or an MLA that is in the custody or control of the Legislative Assembly Office* (section 4(1)(k)):** A record created by or for the office of the Speaker of the Legislative Assembly or the office of a Member of the Legislative Assembly that is in the custody or under the control of the Legislative Assembly Office is not within the scope of the *Act* (see *IPC Order 97-017*).

***Correspondence of Ministers, MLAs and agency heads* (section 4(1)(l)):** This provision excludes certain records created by or for

- a member of the Executive Council;
- a Member of the Legislative Assembly; or
- a chair of a Provincial agency as defined in the *Financial Administration Act* who is a Member of the Legislative Assembly.

In order to be excluded from the scope of the *Act*, the record must have been sent, or be intended to be sent, to another Minister or MLA, as defined above (see *IPC Order 97-007*).

This provision recognizes situations such as those that arise with Standing Policy Committees, where information that may eventually form part of the discussions of the Executive Council, the Treasury Board or one of their respective committees is exchanged and is the subject of discussion, consideration, advice and recommendation.

It also covers situations where the chair of a board or agency is an MLA. Examples include the Seniors' Advisory Council and the Northern Alberta Development Council.

The exclusion extends to copies of such records sent to others, including officials in a public body (see *IPC Order 99-005*).

***Alberta Treasury Branch records* (section 4(1)(m)):** Records in the custody or under the control of an Alberta Treasury Branch other than a record that relates to a non-arm's length transaction between the Government of Alberta and another party, are excluded from the coverage of the *Act*.

This provision protects the banking records of individuals, corporations and organizations that deal with the Alberta Treasury Branches.

In order for this exclusion to apply, the record must be in the custody of the Alberta Treasury Branch or under its control. The Treasury Branch must either have possession of the original record or some authority to manage it (see *IPC Order 98-019*).

A *non-arm's length transaction* is defined, for the purposes of this provision, and the following provision concerning credit union records, as any transaction that has been approved by:

- the Executive Council or any of its committees;
- the Treasury Board or any of its committees; or
- a member of the Executive Council (**section 4(3)**).

This definition does not apply to **section 15** of the *Act* (see *IPC Order 98-013*).

***Credit union records* (section 4(1)(n) and (o)):** The following records relating to credit unions are excluded from the *Act*:

- records relating to the business or affairs of Credit Union Central Alberta Limited, a credit union or a dissolved credit union; and
- records relating to an application for incorporation as a credit union.

In both cases, the records must be obtained or produced in the course of administering or enforcing the *Credit Union Act* or the regulations under it, and must relate to a transaction that is not a non-arms length transaction as described above.

A record of information referred to in section 119(3) of the *Credit Union Act* (advertising of long-term unclaimed balances) or respecting loans made by a credit union that are subsequently assumed by the Credit Union Deposit

Guarantee Corporation are also excluded.

Many of these types of records are dealt with extensively in *IPC Order 97-003*.

Dealing with Excluded Records

Where excluded records or information form a portion of the records responsive to a FOIP request, a public body should consider whether the request for access to the information could be accommodated outside the FOIP process.

If the public body decides to disclose these records, the response to the applicant should explain that the records are excluded from the *FOIP Act*, and that the public body has decided to provide them outside the FOIP process in this case. The response should also explain that the Information and Privacy Commissioner has no jurisdiction over records that do not fall within the scope of the *FOIP Act*.

Where an excluded record or part of a record forms a portion of the records responsive to a request and will not be disclosed, the public body should indicate that the record, or part of the record, is excluded.

The public body should also consider whether any exceptions in the *Act* apply to the information.

If there is a request for review by the Information and Privacy Commissioner, and the Commissioner finds that the information is not excluded, an opportunity will be given to the public body to consider any exceptions that may apply. See *IPC Practice Note No. 4, Section 4 – Exclusions from the Act*.

Dealing with Paramount Legislation

Section 5(2) of the *Act* states that if a provision of the *FOIP Act* is inconsistent or in conflict with a provision of another enactment, the provision of the *FOIP Act* prevails unless another Act or the FOIP Regulation expressly provides that the other enactment prevails.

If a provision of another Act or Regulation is paramount over the *FOIP Act*, then the *FOIP Act* does not apply, *to the extent of the conflict or inconsistency*.

The relationship of the *FOIP Act* to other legislation is discussed further in Chapter 4.2 of this publication.

1.8 ACCESSING INFORMATION

There are three methods for the public to gain access to the information and records of public bodies:

- routine disclosure in response to inquiries and requests for information;
- active dissemination by the public body; and
- FOIP requests.

Routine disclosure and active dissemination, which are described in sections 1.9 and 1.10 of this chapter, will likely satisfy most of the information needs of members of the public. Public bodies should bear in mind that **the FOIP process is in addition to and**

does not replace existing procedures for access to information (section 3(a)).

Public bodies will find it beneficial to undertake continuous review of their processes and channels for providing information and records to the public to ensure that they are operating effectively and in support of the *FOIP Act*.

1.9 ROUTINE ACCESS TO INFORMATION

All public bodies provide routine access to information to members of the public. The *Act* does not replace existing procedures for providing access to information (see section 1.4 of this chapter). Most information should be made available as a matter of ordinary business.

Indeed, the *Act* is intended to strengthen these informal access rights by encouraging routine disclosure and requiring public bodies to provide access to decision-making manuals (**section 84(1)**). FOIP requests should be the last resort for someone seeking information from a public body.

FOIP requests are time-consuming and expensive to process. The more information that can be released to the public or interested segments of the public through normal channels, the more effective a public body will be both in administering its programs and activities and in meeting the spirit of the *FOIP Act*.

There are a number of ways that public bodies currently make information accessible through regular channels, without the need for a FOIP request.

***Answers to particular questions*:** Public bodies handle a large number of inquiries from members of the public seeking the answer to a question rather than asking for access to records.

Occasionally, a person will combine a question with a request for records. To the greatest extent possible, public bodies should continue to deal with these questions without a FOIP request through information offices or the appropriate program area and approval process.

Only when it becomes clear that the request involves records that cannot be released outside the FOIP process, such as personal information about a third party, should the person be referred to the formal process under the *FOIP Act*.

***Reports and publications*:** Much information is available in reports and publications through government websites and through various program information offices. These may either be available free of charge or for a price.

In order to meet the spirit of the *Act*, public bodies should maintain listings of material they publish through their communications office, library, information resource centre or the office of the FOIP Coordinator.

Similar practices should also be adopted for computer databases and information services that are available on various electronic networks. In planning these information dissemination channels, public bodies should consider how such information may be made more available through library and community networks, as well as larger networks, such as the Internet.

***Records available without a FOIP request*:** **Section 83(1)** of the *Act* provides that public bodies may specify categories of records in their custody or under their control that will be made available to the public without a request for access under the *Act*.

In this way, public bodies can take a proactive approach by setting up channels for the release of information and identifying records that are available without a FOIP request.

This approach supports efficient administration, maximizes the use of resources and promotes more openness and accountability in a public body.

Routine disclosure, in response to a routine inquiry or request, occurs when access to a record can be granted without a request under the *FOIP Act.*

Active dissemination occurs when information or records are periodically released, without any request, under a program or release strategy.

Active dissemination is best used where there is a strong and constant demand for information by the public.

Quite often such information is now being mounted and disseminated through database networks or Internet services. Information made available by active dissemination may lend itself to pricing through subscription or dissemination charges or to cooperative dissemination ventures with public organizations or the private sector.

Public bodies might consider the appropriateness of routine disclosure in the following situations:

- disclosure is mandated by another statute or by-law;
- **section 38** of the *FOIP Act* permits disclosure and any conditions specified in **section 38** apply in the circumstances;
- no exceptions to access apply to records;
- any exceptions that apply to a class of records are not mandatory exceptions, and the public body, if it received a request for the particular class of records, would not invoke any discretionary exceptions; or
- exceptions do apply to a class of records but the sensitive information can easily be severed from the other information and that other information may be routinely disclosed.

There are numerous advantages to this type of approach. The public will be better served and better informed through targeted information releases that serve overall program objectives. As well, release of information outside the FOIP process, through a combination of disclosure in response to routine inquiries and requests and active dissemination, can promote cost-effective management of public information resources.

Selecting records for routine disclosure can make it easier for staff to provide information to the public in an efficient manner and to partner with libraries, non-profit organizations and the private sector as agents for disseminating information to citizens and clients.

In addition, **section 83(2)** enables a public body to set fees for the provision of information in this manner, unless records can otherwise be accessed without a fee.

If a request cannot be satisfied entirely through routine disclosure, then the request may be dealt with in part through routine disclosure and in part through the FOIP request process. An example would be a request that requires all records related to a topic rather than just the finished report.

Public bodies should ensure that guidelines are available to all staff of a public body so that they are aware of the types of information that are available for release without a FOIP request. As well, staff should be aware that advice is available from the FOIP Coordinator on this type of disclosure. The Coordinator should monitor the types of requests received by the public body to determine subject areas and records that may qualify for access without a FOIP request or through active dissemination.

Chapter 3 of this publication deals with the processing of FOIP requests.

Special Conditions for Personal Information

Personal information requires special consideration when making decisions about disclosure through routine channels.

Public bodies may be able to identify categories of records containing personal information that may be routinely made available only:

- **to the individual the information is about, or**
- **to the individual's legal representative (section 79(1)).**

Designation of categories of personal information for this limited form of routine disclosure does not require any specific legislative authority.

The public body must, when providing routine disclosure of personal information:

- verify the identity of the person to whom the information is disclosed; and
- ensure that any person exercising the rights of an individual under **section 79** of the *Act* provides appropriate written evidence of his or her right to exercise that individual's rights under the *Act*.

Designation of categories of personal information for routine disclosure to the individual the information is about is appropriate where a considerable demand occurs for a particular type of record. Making the process more routine, with fewer processes and approval requirements, can save a public body considerable time, effort and resources.

Examples include providing routine access to a client's file or to personnel records of an individual. When providing routine access to these kinds of records, public bodies must ensure that disclosure of personal information of other individuals does not occur. Advice from the FOIP Coordinator should be sought on procedures for providing routine disclosure of these records.

Section 83(2) permits public bodies to set a fee for providing records to individual members of the public unless the records can be accessed without a fee. If a process for dealing with requests for information outside the *FOIP Act* is put in place, individuals who make FOIP requests can be referred to the routine process.

However, if there are two processes for obtaining access to information, such that a public body will provide routine access by individuals to their own files in addition to providing access in response to a FOIP request, then the public body should advise individuals of the two processes. Public bodies should ensure that individuals are aware of both their statutory rights under the *Act* and the availability of any other method of access.

Where two processes exist, a public body meets its duty to assist an applicant under **section 9(1)** only if it informs the applicant that such a dual process is in place (see *IPC Order 98-002*).

1.10 PRACTICES FOR ROUTINE DISCLOSURE AND ACTIVE DISSEMINATION

A major challenge for public bodies is to provide information and related client services to the public in a cost-effective fashion. To help satisfy this demand and foster more open public administration, the following practices to support routine disclosures have been developed. These practices are based on the concepts of *routine disclosure* and *active dissemination*, as defined in section 1.8 of this chapter.

***Review of information holdings*:** In starting to establish a system of routine disclosure and active dissemination, it is necessary to review the records of the public body to determine where the concepts may apply.

Examples of release and dissemination include:

- release of particular information whenever a member of the public requests it as part of the service being offered;
- use of public information centres to provide information services, including services by mail and fax;
- use of reference databases to answer queries from clients;
- publication of self-browse and self-service database services;
- distribution of databases to libraries and other public facilities or use of private sector information services to make popular government or local public body databases available; and
- use of the Internet and other public networks to distribute government or local public body records and information.

A list of public information sources for the public body should be prepared, kept up-to-date and distributed to all staff who deal with inquiries from the public. Such information should not need to be dealt with under the access provisions of the *FOIP Act*.

***Coordinating committee*:** Where a public body is large or decentralized, it may be advantageous to develop a network of contacts in program and administrative areas or in its various institutions.

This may be built into a coordinating group that is mandated to develop a corporate policy on routine disclosure and active dissemination and to help implement routine disclosure practices. Members of such a group might include:

- interested individuals from program areas with records that may well qualify for routine disclosure and active dissemination;
- a communications officer interested in information release and dissemination;
- a representative of the records and information management practices area in the public body, who has a good grasp of the types of records held by the public body;
- a representative from the information technology area, who understands how the public body can use new information networks to release and disseminate information and;
- a FOIP Coordinator who understands how routine disclosure and active dissemination can assist the public body in dealing with the demands of the *FOIP Act*.

Either the FOIP Coordinator or the Committee should develop a corporate policy on routine disclosure. Information about what is available routinely from the public body should be made available to client groups and to the public.

***Review of inquiries*:** The FOIP Coordinator or the committee should review the types of requests for information currently made to the public body to determine whether these can be met through either routine disclosure or active dissemination. The objective should be to respond to as many requests as possible outside the *Act*. This should involve an ongoing monitoring and review of FOIP requests to determine whether requests of a particular nature can be handled under routine disclosure practices.

***Review of records*:** There is also a need to review the record holdings of the public body to determine which records not currently subject to routine disclosure or active dissemination may qualify for such procedures. Special attention should be paid to the categories of records set out in section 1.9 of this chapter.

Every jurisdiction that has implemented freedom of information legislation has found that there has been considerable ongoing demand for contracts, travel claims, major reports and plans, internal audits, tax and regulatory rulings, and inspection records, among other types of information.

Attention should be given to these types of records for the application of routine disclosure or active dissemination.

In some instances, records may have to be written and prepared in a different way to facilitate access. For example, reports might be written in a more structured way, such that recommendations or personal information can easily be severed and the remainder of the record made public. Where this is necessary, the public body should establish standards for the creation of these types of documents and ensure that staff are familiar with them.

***Delegation of authority*:** The public body should delegate authority for all routine disclosure to the program area of the organization where the information is collected, compiled or created. The program area or organization should, in accordance with the corporate policy of the public body on routine disclosure, establish mechanisms for the rapid and effective release of the information.

In the case of active dissemination, the program area should be delegated the responsibility and accountability for establishing a dissemination mechanism. The FOIP Coordinator should play an advisory role in establishing such mechanisms, monitoring that action has been taken, and obtaining information on how these mechanisms are working.

A listing of all records subject to routine disclosure and active dissemination should be available to all employees of the public body. They should receive training on assisting the public when a request is made for a record that falls within these categories and on where to refer members of the public when it is unclear whether or not the information may be released.

***Creation of new records*:** The corporate policy on routine disclosure and active dissemination should ensure that the FOIP Coordinator is consulted when there are plans to create new types of records within the public body. This consultation should determine whether or not any of these new records could be subject to routine disclosure or active dissemination.

Consideration should be given, where possible, to modifying standard records by removing segments that would be subject to mandatory exceptions.

For example, if a record contains both general information and personal information, but the main purpose of the record is to provide general information, then practices can be put in place to move personal information on to a separate page or suppress the fields for personal information in an electronic record. This may make the record available for either routine disclosure or active dissemination.

***Channels for active dissemination*:** Active dissemination can take many forms. As indicated above, a public body may have an information centre for clients where information can rapidly be gathered and sent to clients, by mail, fax or through electronic networks. Information may also be routinely made available in a public reading area.

Public bodies can establish Internet sites or on-line databases where interested citizens can obtain information either through an intermediary, or by direct on-line access if they have the necessary equipment and expertise. In other instances, public bodies can use other public or private agencies, including libraries or non-profit organizations that are part of their clientele, or general information services to distribute information on their behalf.

All active dissemination projects involve some investment by public bodies, and these costs have to be balanced against improved services to the public.

Sometimes, public bodies will want to charge fees or collect revenues from the licensing of databases to private electronic publishing services.

When considering active dissemination of electronic products, public bodies should, whenever appropriate and within budgetary constraints, consider using public and local networks such as the Internet, freenets and civic networks.

Chapter 2
Administration of the *FOIP Act*

2.1 PUBLIC BODY – ROLES AND RESPONSIBILITIES

Head of a Public Body

The head of each public body is responsible and accountable for all decisions made under the *FOIP Act* that relate to that public body.

If the public body is a department, branch or office of the Government of Alberta, the head is the member of the Executive Council who presides over the public body (**section 1(1)(f)(i)**).

For other provincial public bodies (agencies, boards, commissions, etc., designated in the FOIP Regulation), the head is the person designated by the Minister responsible for that public body. If a head is not so designated, the person who acts as the chief officer and is charged with the administration of the body is the head (**section 1(1)(f)(i.1)**).

This provision recognizes that small agencies and boards may receive support services from a government department. In these cases, the Minister can assist them by designating a head for the purposes of the *FOIP Act*, for example, from within the department.

For local public bodies, the head is the person or group of persons designated by by-law or other legal instrument to perform the duties of the head for purposes of the *Act* (**sections 1(1)(f)(ii)** and **89(a)**).

In any other case, the head is the chief officer of the public body (**section 1(1)(f)(iii)**).

The governing authority of a local public body will normally designate its chief administrative officer, or equivalent, as head. Examples include a president of a post-secondary educational body, a city or town manager, a head librarian, and a school superintendent. However, the governing authority may decide to appoint a committee to fulfil this role.

Governing authorities of local public bodies must designate a head by by-law or by another legal instrument by which they act.

FOIP Coordinator

The Minister responsible for the FOIP legislation requires each public body to have a key contact person who can deal with FOIP matters.

This function is performed by the FOIP Coordinator. The FOIP Coordinator is responsible for overall management of the freedom of information and protection of privacy function within a public body.

Depending on the size and resources of the public body, the Coordinator may carry out his or her responsibilities on a full-time or part-time basis, or may be someone appointed from outside the public body to carry out FOIP responsibilities on its behalf. Some FOIP Coordinators provide shared services for several public bodies.

The FOIP Coordinator's office should provide the focal point for freedom of information and protection of privacy expertise within the public body. Details of the responsibilities of this office throughout this publication represent a typical delegation of tasks. Public bodies may find that a different distribution of responsibilities is appropriate for them.

The responsibilities include:

- implementing policies, guidelines and procedures to manage the public body's compliance with the provisions of the *Act*;
- providing advisory services to the staff of the public body;
- developing and delivering training programs on freedom of information and privacy protection within the public body and coordinating participation in FOIP courses offered by the Government of Alberta;
- informing the public body's clients, and all those with which it does business or provides services, about the *Act*;
- advising senior management on information that can be released without a FOIP request;
- coordinating the public body's input to the directory of records required by the *Act* and, for local public bodies, establishing a list of personal information banks;
- managing the FOIP request process for the public body, which may include:
  - assisting applicants,
  - assigning requests to program areas,
  - monitoring and tracking the processing of requests,
  - meeting time limits and notification requirements,
  - considering representations from third parties,
  - calculating fee estimates and collecting fees,
  - reviewing preliminary recommendations from program areas, sections or organizations about the release of records and proposals for severing information,
  - making final recommendations on responses to requests, and
  - responding to applicants;
- ensuring that the privacy protection measures in **Part 2** of the *Act* are implemented and carried out on an ongoing basis;
- coordinating any negotiations, mediations, inquiries, investigations, and audits with the Office of the Information and Privacy Commissioner;
- ensuring consistency in the application of other Acts and regulations which relate to the prohibition or restriction on the disclosure of information (**section 5**); and
- reporting as required to the Ministry responsible for FOIP on the operation of the *Act*.

In the case of provincial public bodies, responsibilities also include:

- maintaining a list of the provincial public body's affiliated agencies for the purposes of **Schedule 1** of the FOIP Regulation; and
- consulting with Alberta Municipal Affairs regarding any legislative developments or amendments in other legislation that might relate to the *FOIP Act*.

Program Administrators

In larger or decentralized public bodies, program administrators or department heads have special responsibilities for ensuring effective administration of the *FOIP Act*.

Normally, they are accountable for:

- ensuring that the management of records in the custody or under the control of their program area meets the requirements of the legislation, especially the provisions relating to the protection of privacy;
- identifying and providing access to information that can be released without a FOIP request;
- processing FOIP requests; and
- approving program area recommendations for responding to FOIP requests.

In larger organizations with decentralized FOIP administration, each program should have an appointed program contact to ensure that requests are processed effectively, that information that can be routinely released is identified, and that privacy protection measures are implemented.

Communications

In public bodies with a public relations area, communications staff may have a direct role in the freedom of information and protection of privacy function.

Release of information in response to an access request should be coordinated with the overall flow of information to the public.

Release of information without a FOIP request, active dissemination of information, and publication of information through paper and electronic means should continue to be the normal way of serving those interested in obtaining information.

Where sensitive issues are involved, public bodies may wish to have a communications strategy in place when FOIP disclosures take place.

Records and Information Management

The records and information management function within a public body is a major support for effective administration of the *FOIP Act*. The same is true of the information technology function relating to the control of electronic databases and records.

Each public body should coordinate its efforts for managing, administering, controlling, providing security for, and preserving all its records. This includes electronic data and information, publications and other reports in its custody or under its control. This will ensure that the public body can meet its requirements under the *Act*.

Records and information management supports the FOIP Coordinator in:

- establishing and maintaining an adequate level of information control to ensure that all records can be located and retrieved within the required time limits;
- establishing and maintaining information management systems for

the public body that comply with the *Act*'s privacy protection provisions;
- providing a complete description of records for input into the directory of records required by the *Act* and, for local public bodies, creating a listing of all personal information banks;
- ensuring that records retention and disposition schedules are established, authorized as required, and applied to all information in the custody or under the control of a public body; and
- providing a basis for implementing information security measures for sensitive records and for the reasonable protection of personal information.

Additional guidance on Records and Information Management Practices is provided in Chapter 8 of this publication.

2.2 DELEGATION OF FOIP RESPONSIBILITIES

Under **section 80** of the *Act*, the head of a public body has the power to delegate to any other person any of the head's duties, powers and functions under the *Act*, except the power to delegate.

In a very small public body, where the designated head may also be the FOIP Coordinator, there will generally be no need to delegate. In larger public bodies a delegation instrument will be needed.

The delegation instrument should identify the position, not the individual, to which the powers are delegated. When delegation is to the position rather than the person, a new delegation is not required when a new appointee assumes the position or when someone is acting in the position.

A delegation instrument may also recognize another position to which delegation passes if the occupant of the original position is absent or incapacitated.

A delegation instrument may cover a wide variety of duties, powers and functions, including those under the *FOIP Act* as well as others.

A delegation instrument remains in effect until replaced.

There is a substantial difference between delegations relating to freedom of information and those relating to protection of privacy.

In the case of freedom of information, the delegations relate mostly to the processing of an access request and the decision whether or not to release all or part of a record. Delegated authority empowers certain officials and employees to make decisions or take action.

In the case of privacy protection, responsibilities centre on the collection, handling and protection of personal information. This is a much more general area of responsibility and is centred on the program areas or local offices that handle the information on a day-to-day basis. Even in small public bodies, privacy protection responsibilities should be delegated to line staff responsible for the information.

Not every section of the *Act* dealing with privacy matters calls for delegation of responsibility in a formal sense. The head of a public body should, however, clearly advise program administrators and managers of their responsibilities, especially with regard to compliance in the collection and disclosure of personal information.

In general, delegation should be considered for all provisions of the *Act* that state that the head of a public body may or must do something. A **Delegation Table** that lists all the provisions of the *FOIP Act* for which delegation should be considered is provided in Appendix 2 of this publication. Public bodies need to customize this listing to their actual operations. This includes using the organization's own position titles and providing for delegation to multiple positions where appropriate.

The delegation table makes provision for the identification of specific officials by title and office (e.g., the Executive Manager, Personnel) and for generic titles such as "all program managers." It is essential when a delegation instrument is put in place that all identified officers or employees know and understand their responsibilities.

Job orientation materials should also include a statement about FOIP responsibilities for each official or employee taking up a position that includes delegated responsibilities under the *Act*, and an indication that additional information can be obtained from the FOIP Coordinator.

The nature of actual delegation is very much determined by the structure of the public body and the approach that it wishes to take toward administration of the *FOIP Act*.

Delegation is decided in consultation with elected officials or governing board members and senior management in the public body. In smaller public bodies, for instance, the head may choose to delegate to a single officer or person. In larger public bodies or in decentralized organizations, however, the head may wish to spread decision-making responsibilities more widely to department heads or below.

The FOIP Coordinator normally prepares the delegation instrument and submits it to the head of the public body for approval.

2.3 PROVINCE-WIDE ADMINISTRATION OF THE *ACT*

Minister Responsible for FOIP

The Lieutenant Governor in Council designates the Minister responsible for the *Act* by Order in Council. The Minister of Municipal Affairs has been given this responsibility.

The Minister has overall responsibility for the general administration of the *Act* across the province, including preparation and submission of amendments to the *FOIP Act* and FOIP Regulation and providing guidance about FOIP.

The Minister is required to report annually to the Legislative Assembly on the administration of the *Act* (**section 81**).

The Minister is also responsible for publishing information to assist the public in identifying and locating records, including records in personal information banks. This is required under **section 82** of the *Act*.

Information Management and Privacy, Alberta Municipal Affairs

Information Management and Privacy supports the Minister responsible for FOIP in all aspects of the implementation and administration of the legislation across all public bodies.

Information Management and Privacy provides public bodies with the following services and products:

- the development and distribution of regulations, policies and guidelines where appropriate or needed to assist public bodies in administering the legislation;
- advice and guidance on the interpretation, implementation and operation of the *Act* and Regulation, including a "help desk" to deal with implementation issues;
- regular posting and distribution of updated FOIP legislation and policies, as well as orders issued by the Information and Privacy Commissioner and other information – both in print and on the Information Management and Privacy web site;
- a computer-based tracking system for FOIP requests and statistical reporting which may be used by public bodies;
- guidelines and assistance in the development of entries for directories of records and, for local public bodies, the listings of personal information banks;
- organization of regular FOIP training sessions and seminars;
- production of publications to enable FOIP Coordinators, key contacts and others in public bodies to remain up-to-date on issues and trends in the fields of freedom of information and the protection of privacy; and
- guidelines on information that must be reported by public bodies to support the preparation of the annual report.

Key Departments

There are a number of departments that have statutory responsibilities relating to particular local public bodies. These include the provincial ministries of Municipal Affairs, Learning, Health and Wellness, Justice, International and Intergovernmental Relations, and Community Development.

Key departments assist local public bodies in resolving implementation and administration issues regarding the *Act*.

Key departments are also partners with Information Management and Privacy in answering questions, resolving implementation issues, sponsoring meetings and other training forums, and providing speakers in the area of freedom of information and protection of privacy.

Information and Privacy Commissioner

The Information and Privacy Commissioner is an Officer of the Legislature who is independent of government. The Commissioner is responsible for providing an independent review of decisions made under the *Act* and issues orders in that capacity.

The Commissioner reports annually to the Speaker of the Legislative Assembly on the operation of the legislation (**section 61**).

The powers of the Commissioner and the role of the Office of the Commissioner are discussed in Chapter 10 of this publication.

2.4 LIABILITY, SANCTIONS AND PENALTIES

Protection from Liability

Under **section 85** of the *Act*, a public body and all the officials involved in the administration of the *Act* are protected from liability for damages for:

- disclosing or withholding information, or for the consequences of disclosing or withholding information, where a public official has acted in good faith; or
- failing to give a required notice where the public official took reasonable care in giving notice.

Section 85.1 protects an employee of a public body from adverse employment action as a result of properly disclosing information in accordance with the *Act*.

Anyone who violates **section 85.1** is guilty of an offence and liable to a fine of not more than $10,000.

Offences and Penalties

Section 86 of the *Act* requires public bodies to cooperate both with the Information and Privacy Commissioner or another person conducting duties of the Commissioner under the *Act*.

It is an offence to:

- collect, use or disclose personal information in violation of **Part 2** of the *Act*;
- attempt to gain or gain access to personal information in violation of the *Act*;
- make a false statement to or mislead or attempt to mislead the Commissioner or another person in the performance of the duties, powers or functions of the Commissioner or another person under the *Act*;
- obstruct the Commissioner or another person in the performance of the duties, powers or functions of the Commissioner or other person under the *Act*;
- alter, falsify or conceal any record, or direct any person to do so, with the intent of evading a request for access under the *Act*;
- fail to comply with an order made by the Commissioner under **section 68** or by the adjudicator under **section 76(2)**; or
- destroy any records subject to the *Act* with the intent to evade a request for access to the records.

Failure to comply with a duty imposed by the legislation or otherwise acting in contravention of the *Act* is not an offence unless it is covered under **section 86(1)**.

The Commissioner may find grounds for believing that an offence under **section 86(1)** has occurred in the course of:

- a review requested by an applicant or other individual under the *Act*,
- an investigation under **section 51,** or
- a disclosure to the Commissioner under **section 77** regarding possible

failure to disclose in the public interest or violation of **Part 2** of the *Act*.

Any other failure to comply with the legislation that is not an offence under **section 86(1)** is dealt with by the Commissioner under the normal review and complaints process set out in **Part 4** of the *Act* or in an investigation under **section 51**.

Any person who commits an offence under **section 86(1)** or **section 85.1(1)** is liable, upon conviction, to a fine of up to $10,000 under **sections 86(2)** and **85.1(2)** respectively.

The Commissioner does not impose the fine. The court would determine whether or not an offence had been committed and impose any fine.

Chapter 3
Access to Records

3.1 WHO HAS A RIGHT OF ACCESS

Under **section 6(1)** of the *FOIP Act*, any person has a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the applicant.

There are no restrictions on who may make a request. The applicant can be any person inside or outside Alberta, including individuals, corporations, and organizations. The *Act* does not specify a minimum age, which means that minors may make requests.

3.2 ACCESS TOOLS

Directories of Records

In order to provide for effective access to records in the custody or under the control of public bodies, it is important that the public is able to obtain information to assist in identifying and locating records.

Section 82(1) requires the Minister responsible for the *Act* to ensure that this information is made available.

The directory of records should include:

- a description of the mandate and functions of each public body and its components;
- a description of the records in the custody or under the control of each public body;
- a general listing of records in the custody or under the control of each provincial public body;
- a subject index;
- the title, business address and business telephone number of the head of the public body; and
- the address of any office of the public body authorized to receive requests (see **section 82(2)** of the *Act* and **section 2(1)** of the FOIP Regulation).

For each personal information bank, provincial public bodies are required to provide:

- the title and location of the personal information bank;
- a description of the kind of personal information and the categories of individuals whose personal information is included;
- the authority for collecting the personal information;
- the purposes for which the personal information was collected and the purposes for which it is used or disclosed; and
- the categories of persons who use the personal information or to whom it is disclosed (**section 82(3)**).

A *personal information bank* is defined as a collection of personal information that is organized or accessible by the name of an individual or by an identifying number, symbol or other particular assigned to an individual (**section 82(9)**).

Personal information banks have the following characteristics:

- they contain one or more types of personal information;
- they contain information about a group or groups of individuals; and
- the information is organized by a personal identifier or capable of being retrieved by a personal identifier.

Collections of information that are neither organized nor accessible by an identifier that is personal information do not qualify as personal information banks, even if the collection contains personal information. Information that is retrievable only by corporate name does not constitute a personal information bank. Nor does a list of non-profit organizations where there is no index or capability of retrieving the names of the contact officers.

The listing of personal information banks provides a public registration of all personal information banks in the custody or under the control of a public body. It also provides a public record of the purposes for which this information may be used or disclosed.

The Information and Privacy Commissioner may consider or review a public body's listing of personal information banks if there is a complaint or general investigation relating to the collection, use or disclosure of personal information by a public body.

Further information about personal information banks is available in two guides published by Information Management and Privacy, Alberta Municipal Affairs. They are: *Identifying Personal Information Banks: A Guide for Local Public Bodies*, and *Identifying Personal Information Banks: A Guide for Provincial Government Ministries*.

Special Conditions for Local Public Bodies

Local public bodies are required to provide to the public a description of their mandate and functions and a general description of the records in their custody or under their control (**section 82(5)**).

Each local public body is also required to make available, for inspection and copying by the public, a directory that lists its personal information banks and includes:

- the title and location of the personal information bank;
- a description of the kind of personal information and the categories of individuals whose personal information is included; and
- the authority for collecting the personal information (**section 82(6)**).

Accessing Manuals and Guidelines

Section 84(1) of the *Act* requires that public bodies make available for inspection by the public any manual, handbook or other guideline used in decision-making processes that affect the public. This provision applies to manuals used by employees while administering or carrying out programs or activities.

Rules for program administration, formulae or eligibility criteria for grants or other benefits, guidelines for reviewing applications, and procedures for administering a public program are included.

This availability of material that guides decision-making allows members of the public to understand how decisions that affect them are made and opens up the decision-making process to public scrutiny.

Manuals or handbooks that deal only with internal decision-making, such as internal personnel practices or records management guidelines are not included.

Each public body should provide facilities where the public may inspect this information, both at its headquarters and, if reasonably practicable, at other offices of the public body.

There are a number of ways to accomplish this. One approach may be to designate space in the office areas of the FOIP Coordinator and appropriate regional contacts. Another is to provide access in an existing library or resource centre.

The term *facility* may include locations such as a reception area, a workstation, an office or any other area set aside for this purpose. In all cases, however, the location should be clearly indicated so that the public may easily locate it.

At a minimum, public bodies should be able to produce, on request, copies of all manuals, handbooks and guidelines that have been prepared for public inspection.

Section 84(2) provides that manuals, handbooks and guidelines may be reviewed by the public body before being made available for public examination. Any information that should not be disclosed in accordance with the exception criteria set out in the *Act* may be severed.

If information is severed, the record must include a statement that information has been severed, a description of the general nature of the severed information and the reason for the severing.

Accessing manuals and guidelines and the establishment of facilities for the public to consult these documents is discussed in *FOIP Bulletin No. 3, Manuals and Reading Rooms*.

3.3 RECEIVING A FOIP REQUEST

Nature of Request

Section 7(1) of the *Act* provides that an applicant must make a request to a public body that the applicant believes has custody or control of the particular record(s).

Section 7(2) requires that the request be in writing and provide enough detail to enable the public body to identify the record.

Applicants may request either to examine the record or to obtain a copy of it (**section 7(3)**). As long as the original request was properly made, a change to the original terms of the request, for example, where the applicant asks to examine records rather than to receive copies, may be verbal (see *IPC Order 99-011*).

The initial fee of $25.00 for a one-time request or $50.00 for a continuing request must accompany a request for general records. There is no initial fee when the applicant is requesting his or her own personal information. No GST is charged for FOIP requests.

Form of Request

The applicant can use the official request form. A copy of the **Request to Access Information Form** can be found in Appendix 6 of this publication.

Public bodies may either use this form or create one of their own.

Alternatively, an applicant may simply write a letter, requesting records and referencing the *FOIP Act*.

Alternative Forms of Access

Section 4 of the FOIP Regulation establishes that:

- an applicant with limited ability to read English; or
- an applicant with a physical disability or condition

may make an oral request.

Public bodies should assist individuals seeking records under the *Act* who are disabled, do not have literacy skills or are otherwise unable to exercise their rights under regular procedures.

In the case of individuals with a hearing impairment, telecommunications devices for the deaf (TDD) should be used. For provincial public bodies, use should be made of the RITE System's toll free number 1-800-232-7215, and in Edmonton 427-9999, as a telecommunications device for the deaf.

For visually impaired applicants, consideration should be given to helping the applicant in making a request by assisting in filling out a request form.

In the case of applicants lacking the literacy skills needed to make a written request, the public body should assist the individual in putting an oral request into written form.

A public body only needs to deal with a request in a language in which the body normally conducts business.

There will also be cases of individuals who live in remote areas and are disadvantaged in comparison with other members of the public in their ability to make a FOIP request. Public bodies should take such situations into account and assist applicants in ways that will enable them to exercise their access rights without excessive cost or delay.

Duty to Assist Applicants

Section 9(1) of the *Act* requires the head of each public body to make every reasonable effort to assist applicants, and to respond to each applicant openly, accurately and completely.

This is an important duty and should be kept in mind throughout the request process. It is critical during the applicant's initial contact with a public body. The FOIP Coordinator and staff should attempt to develop a working relationship with the applicant to define the nature and scope of the request and determine the steps involved in processing the request. **A public body must make every reasonable effort to identify and locate records responsive to a request, and provide the applicant with information regarding the processing of the request in a timely manner.**

Both parties have an interest in the efficient, timely processing of requests. When a FOIP request can be dealt with outside the *Act*, a public body should return to the applicant any fees paid and provide copies of the requested record. Procedures for responding to a request outside the *Act* are discussed in section 3.4 of this chapter.

Acknowledging Receipt of Request

The public body should acknowledge receipt of a request. This acknowledgment may indicate that the request:

- has been received and processing will commence;
- is incomplete because the initial fee has not been paid and is required before processing can commence; or
- is not clear or precise enough and more information is needed to clarify it before processing can commence.

If processing cannot begin immediately, an effort should be made to contact the applicant by telephone to resolve any problems quickly.

A written follow-up to this call is good practice. It will provide a definite reference point as to when processing commenced and a statement of the agreement between the public body and the applicant as to the nature and scope of a request that has been clarified.

Model Letter A in Appendix 3 sets out various options for acknowledging receipt of a request.

Continuing Requests

Section 8 of the *Act* provides that an applicant may ask that a request continue in effect for a specified period of time up to two years. This permits the applicant to continue to receive records concerning a particular subject or issue over time.

The head of the public body may choose to accept or reject a continuing request.

Grounds for rejecting a continuing request may include the following:

- the situation or event that is the subject of the request is not an ongoing matter and there is no basis on which to set up a continuing request; or
- the situation that is the subject of the request is dependent on other actions involving the applicant and the applicant is receiving the information routinely on an ongoing basis.

The *Act* applies to a continuing request as if a new request were received on each of the dates on which processing of an instalment of the request is due to begin. The public body is required to provide the applicant with a schedule indicating the series of dates when the request will be deemed to have been received and to inform the applicant that he or she has the right to ask the Commissioner to review the schedule.

On each scheduled date, the time limit for responding to the request begins again. **The FOIP Coordinator should have a system in place to alert the office when a request should be reactivated.**

Model Letters A and **B** in Appendix 3 deal with continuing requests.

Request for Personal Information about an Applicant

Individuals may also make requests for information about themselves. **The same general conditions apply to receiving these requests except that no initial fee is required.**

It is usually obvious from the face of the request that someone is requesting his or her own personal information. In some instances, however, someone else may be applying on behalf of the individual and it will be necessary to determine whether the applicant has the authorization of the individual involved or some other right under the *Act*. Common examples of persons who might reasonably request information about another individual are the legal representative of the individual, and the parent of a young child.

At times it may not be clear whether an applicant is requesting his or her own personal information or general records about a subject in which the individual has been involved.

The Information and Privacy Commissioner dealt with this issue in *IPC Order 97-003*. A three-part test was applied, which proposed that the public body:

- consider the wording of the request;
- characterize the request as to whether it is primarily for general records or is for personal information about the applicant; and
- decide whether the records relate to and are responsive to the request being made and whether the preponderance of records relates to the individual.

On this basis, the public body decides whether or not it is dealing with a request for personal information.

For further guidance on requests by representatives of individuals who may be empowered to seek personal information on behalf of an individual, see Chapter 7.13 of this publication.

Permission to Disregard Requests

In rare instances, a public body may ask the Information and Privacy Commissioner to authorize the public body under **section 53** of the *Act* to disregard certain requests. The head may be allowed to disregard a request if it is:

- repetitious or systematic in nature, and
- processing the request would unreasonably interfere with the operations of the public body, or amount to an abuse of the right to make requests;

or

- frivolous or vexatious.

A request is *repetitious* if it is one in a series of requests by an applicant for substantially the same information or records.

A request is *systematic* in nature if it is part of an extensive pattern of related requests by an applicant or a group of applicants.

A request may be *frivolous or vexatious* if it has no sound basis in fact or is malicious. Public bodies should take into account whether there is a past pattern of conduct that indicates an abuse of the process for access and whether or not the request is made in bad faith or for a purpose other than to obtain access to information.

Examples of requests that might be considered frivolous or vexatious include:

- continual requests for records that a public body has already established it does not have;
- requests involving fees made by an applicant who has demonstrated a pattern of abandoning a request whenever a fee waiver is not granted or the Commissioner upholds a fee; and
- requests that show an intention to harass a public body, to "break" the system or to engage in "information warfare."

Although not binding in Alberta, guidance on such requests can be found in Ontario *IPC Order M-850.*

The onus is on the public body making a request for authorization to disregard a request under **section 53** to make the case to the Commissioner.

More information on this provision can be found in Chapter 10.9 of this publication.

Clarifying Requests

Vague or overly general requests may increase workloads and lead to review of information that is of little interest to the applicant. Often requests are broad or vague because the applicant lacks knowledge of the public body, its mandate and programs and the type of records available.

The FOIP Coordinator should establish contact with the applicant to better understand what information will satisfy the applicant's needs.

If a request does not sufficiently describe the records sought, a public body should advise the applicant and offer assistance in reformulating the request.

Model Letter A in Appendix 3 deals with this type of situation.

There are several things to keep in mind when seeking to define or clarify a request.

Release of information outside FOIP: It is important to verify whether or not the information needs of the applicant can be satisfied by providing records that are already publicly available or that can be made available through a process of routine disclosure. If this is the case, then the relevant information should be released to the applicant without delay.

The applicant should be advised that such information is available without a FOIP request and that there is no need to make an application under the *Act* for similar information in the future.

In some instances, only part of the information can be routinely released. In such cases, this information should be released and the rest of the request processed under the *Act*.

Narrowing a request: It is important to discuss with the applicant any request that involves a vast amount of information. An example would be a request for all the records concerning planning in a public body. The objective is to narrow the request while still meeting the applicant's information needs. This can result in a reduction of fees and provision of better service, in terms of both time and results.

Changing the scope: After discussion of the nature of a request, an applicant will sometimes change the scope of the request. When this occurs, the public body should document the change and send a notice to the applicant (see **Model Letter A** in Appendix 3).

Time limits: The *Act* establishes a time limit of 30 calendar days to respond to a request. The time period begins on the day following receipt of a FOIP request. A request is complete if it mentions the *Act*, is signed and includes the initial fee, if required.

The time period begins when an authorized office receives a request, even when the request is vague and imprecise. An effort should be made to help the applicant to clarify the request, although this cannot be an endless task.

Time extension: When an applicant will not narrow or be more precise in a request, or when a request is genuinely broad in nature, **section 13(1)(a)** enables the public body to extend the time for responding to a request for another 30 days (allowing a total processing time of 60 calendar days).

More information is given about extensions of time limits below, under the heading Response Time Limits.

Documenting and Tracking Requests

All public bodies should maintain documentation systems to record all deliberations and decisions regarding the processing of requests and to help ensure that the request process meets the requirements set out in the *Act*.

This documentation may become a critical part of the evidence required during a review by the Information and Privacy Commissioner. It can also be of assistance in the processing of subsequent similar requests (see *IPC Order 99-011*).

As provided in **section 2** of the FOIP Regulation, the 30-day time period for responding to requests commences on the day after receipt of a request in the office of the public body designated to receive such requests. This is normally the office of the FOIP Coordinator.

Authorized offices are listed in the directory published on the web site of Information Management and Privacy, Alberta Municipal Affairs (www.gov.ab.ca/foip) and may be publicized in other ways. Authorized offices are usually the offices of the head of the public body and the FOIP Coordinator.

A request may be delivered to any office of a public body during normal business hours, but the time limit for responding to the request does not commence until the request is received in an office authorized to receive requests.

Section 2(3) of the FOIP Regulation requires the public body to have a reasonable system in place to ensure that FOIP requests are forwarded immediately to the office(s) designated to receive and begin processing them.

Reasonable steps might include special forwarding instructions to staff in mail rooms within the public body and to staff that open the mail, as well as use of a colour-coded transmittal file to indicate the priority and important nature of the document. Most importantly, staff should be aware of the urgent nature of FOIP requests and the need to forward them immediately to the FOIP Coordinator.

Offices designated to process FOIP requests should date-stamp all requests on receipt.

Public bodies may choose to establish an automated or manual tracking system. The choice will depend largely upon the volume of work generated by FOIP requests.

Automated systems are not normally needed unless a public body receives more than 50 requests annually or the public body is decentralized and there is a need to coordinate responses.

If a decision is made to use an automated system, public bodies may use the tracking system available from Information Management and Privacy, Alberta Municipal Affairs.

When implementing or designing a system, public bodies should keep in mind that information is needed for reporting to the Legislative Assembly by the Minister responsible for the *FOIP Act* on the operation of the *Act*.

Notices regarding reporting requirements are regularly issued to public bodies by Information Management and Privacy, Alberta Municipal Affairs.

Transferring a Request

There are occasions when an applicant makes a request for information to one public body that would be more appropriately handled by another public body. In order to meet the applicant's information needs, it may be better to have the public body that has the greater interest in a record process the request.

Transferring the request to that public body will ensure that people who are familiar with the information are involved in processing the request and that decisions on disclosure are made in the most appropriate context.

Requests for correction of personal information may also be transferred if the information was originally collected, or the record created, by another public body.

The public body originally receiving the request should make every reasonable effort to assist the applicant by identifying the location of the information. This includes ensuring that the public body best able to handle the request receives it.

If the FOIP Coordinator is aware that part of a request relates to records of another public body, the public body receiving the request should inform the applicant that he or she can make a request to the other organization for the information.

***Transfer procedure*: Section 14(1)** of the *Act* provides that within 15 days after receipt of a request a public body may transfer a request, and, if needed, any records relating to it, to another public body if:

- the record was produced by that body;
- the other body was the first to obtain the record; or
- the record is in the custody or under the control of the other public body.

Before a public body transfers a request to another public body, it must ensure that the other public body has a copy of the record and that it agrees to the transfer.

A public body may decline to accept a transfer if the requested record has little or no connection to its duties and functions or it believes the receiving body has a greater interest in the record.

In many cases, interest in the disclosure of particular records will exist in several public bodies. This might be the case, for example, with requests for the records of interdepartmental or multi-organizational committees, or requests for records relating to budgeting processes and programs in which two or more public bodies are involved.

For the sake of administrative simplicity and good client service, the public body receiving such a request should process it, consulting and seeking advice from the other interested bodies, rather than attempting to negotiate a complicated sharing of the request.

In such cases, the public body processing the request has the final decision as to what will be released.

In the case of multiple requests to several provincial public bodies for similar records, each public body should process the request that it has received, in consultation with the other public bodies and Information Management and Privacy, Alberta Municipal Affairs.

Information Management and Privacy may provide a coordinating function for similar requests directed to a number of provincial public bodies. Such coordination involves explaining difficult issues and promoting communication among public bodies. Decision-making about a request will always remain with the public body processing a request.

Section 35.1 of the *Act* provides that a public body may transfer a request to correct personal information if:

- the personal information was collected by another public body; or
- another public body created the record containing the personal information.

This ensures that the public body that originally collected or compiled the personal information makes the corrections, annotation or linkage required. The onus is then on that public body to inform others to whom the information has been disclosed of its decision about the request.

***Conditions of transfer*:** When a request is transferred, **sections 14(2) and 35.1(2)** of the *Act* require:

- the public body that transferred the request to provide notice to the applicant as soon as possible. **Model Letter C** in Appendix 3 deals with the transfer of a request; and
- the public body receiving the request to make a reasonable effort to process the request within 30 days after receiving it, unless a time extension is sought under one of the conditions set out in **section 13** of the *Act*.

The public body to which the request is transferred should also acknowledge receipt of the request by writing to the applicant using **Model Letter A**.

Consultation

When a public body receives a request that deals with records that originated in another public body or deals with matters in which another public body has a direct interest, it should consult with that public body. This will ensure that all relevant factors are taken into consideration in deciding whether or not to disclose all or part of the records.

Two public bodies may deal with different aspects of the same matter or policy and may even disagree on policy directions or administrative actions to be taken. The public body receiving the request should ensure that the views of the other body have been taken into consideration in any decision to disclose or to refuse access to all or part of the records concerned.

If more than two public bodies are involved, the consultation process should ensure that all parties are aware of each other's views.

Public bodies that regularly need to consult with other public bodies on disclosure in response to access requests may need to set out their procedures for consultation and decision-making in policy.

Response Time Limits

Section 10(1) of the *Act* provides that public bodies must make every reasonable effort to respond to a request no later than 30 calendar days after receiving it, unless:

- the time limit is extended under **section 13**; or
- the request is transferred to another public body under **section 14**.

Every reasonable effort means the effort that a fair and rational person would expect to be made and would find acceptable. A public body's effort is expected to be thorough and comprehensive (see *IPC Order 98-002*).

The 30-day time limit is based on calendar days. The time limit begins on the day after the request is received in an office duly authorized to deal with it and any initial fee is paid. See the definition of *time limit* in Appendix 1 of this publication for an explanation of the way time is calculated.

If the request is incomplete and further information is required from the applicant in order to identify the records sought, a public body should seek this information immediately. The requirement to clarify the request does not change the date on which the time period commences, but may necessitate a time limit extension.

***Deemed refusal*:** **Section 10(2)** of the *Act* clearly establishes that the failure by a public body to respond to a request within the 30-day time limit, or a time limit extended under **section 13**, can be treated by the applicant as a decision to refuse access to the record(s). Failure to respond to a request may be reviewed by the Commissioner.

***Time limit extensions*:** **Section 13** of the *Act* provides authority for extending the time limit for responding to a request. The circumstances in which an extension is permitted are limited and, in some cases, the permission of the Commissioner is required.

A public body may extend the time limit for responding by up to 30 days, allowing a total period of up to 60 days, in the following circumstances.

- The applicant does not give enough detail to enable the requested records to be identified. This may be because the request is vaguely worded or, for some other reason, the record is impossible to locate from the description provided. In this case, clarification is needed from the applicant.

- A large number of records is requested or must be searched, and responding within 30 days would unreasonably interfere with the operations of the public body. This type of request will usually result in discussions with the applicant to try to narrow the scope of the search. This provision does not apply to review of the records in order to make a decision on disclosure but only to the search for and retrieval of the records.

- More time is needed for the public body to consult with other public bodies, other levels of government or third parties. This provision applies to third party consultations as required under **section 29** of the *Act* (which may take up to 20 days), consultation with other governments under **section 20** (for which there is no specified time limit), and consultation with other public bodies (where the public body has no legislated power to compel a timely response).

If a public body believes that it still cannot complete processing of the request within a 30-day extension period, it may ask the Commissioner for a longer extension.

Section 13(1)(d) allows for a time limit extension when a third party asks the Commissioner to review a head's decision on a request. In order to allow time for the third party to ask the Commissioner to review the decision, an additional 20 days may be required.

If a review by the Commissioner is requested by a third party, the information must be withheld until the review is completed and any order issued. This provision also applies to situations where an adjudicator may have to be appointed to conduct a review.

Section 13(3) allows the head of a public body to extend the time limit for responding to a request in accordance with individual provisions of the *Act*, without seeking the permission of the Commissioner, even if the cumulative effect of granting allowed extensions takes the time period beyond 60 days. This may occur if the need to consult with a third party is not recognized until late in the processing of a large request.

This provision also protects the rights of third parties to seek a review of any decision to release information about them.

The public body should consider all factors relating to the possibility of the need for a time limit extension before finally deciding to invoke one. Common factors include:

- the amount and type of detail required from the applicant to clarify a request;
- the breadth and complexity of the request, the number of records requested and the number of files that must be searched to find the requested records;
- the number and complexity of consultations required with external organizations, such as other public bodies or other levels of government;
- the quantity and type of records requiring review by other public bodies. The *Act* does not regard other public bodies as third parties for the purposes of notices under **sections 29** and **30.** Consultation with other public bodies is therefore not subject to specific time limits, but they should agree to respond as expeditiously as possible; and
- the amount of time needed for the Commissioner to deal with a request for review. The Commissioner's office should be consulted on this matter.

The *Act* does not provide for extensions for other administrative reasons, such as:

- consultations within the public body after the records have been located;
- line-by-line review of the records after they have been located;
- working conditions arising from sickness, staff absence or vacation, or staff workloads.

***Limits on extensions*:** Public bodies should make every effort to plan the processing of complicated requests so that there is a need to invoke only one extension. A public body may, on its own authority and *within* the original 30-day time limit, extend the 30-day limit for another 30 days or as required to enable the head to comply with requirements of **section 30**.

If the public body believes that responding to the request will require more than a total of 60 days, the head is required to ask the Commissioner for permission to extend the time limit beyond the original 30 days. This must be done in writing and normally within the original 30-day time limit. The reasons for the extension must meet the conditions of section 13(1), as listed above.

For example, if a public body believes that it will take 90 calendar days to process a request, it should request permission from the Commissioner.

within the 30-day original time period, to extend the response time for 60 calendar days (30 original days + 60 day extension = 90 days).

A letter requesting an extension by the Commissioner should set out the specific reasons why a period greater than 60 days is required to process the request.

The letter should propose a reasonable period of days for producing a response.

Normally, if a public body has already taken a 30-day extension under its own authority, it should not seek a second extension from the Commissioner. However, this may be done in exceptional circumstances, where complications not originally contemplated when planning the response process arise.

An example might be where a public body has already claimed an extension of 30 days because of the need for extensive consultation. On the 45th day, as a result of that consultation, it discovers additional records that have to be searched and from which responsive records will be retrieved.

In this case, the public body would request the permission of the Information and Privacy Commissioner to extend the period for response to the applicant.

Section 13(2) of the *Act* also provides for a public body, only with the Commissioner's permission, to extend the time limit for responding to a request in the following circumstances:

- multiple concurrent requests are made by the same applicant; or
- two or more applicants who work for the same organization or who work in association with each other make multiple concurrent requests.

This provision acknowledges the difficulty that a public body may have if one or more applicants make a number of requests at the same time.

It recognizes that the same factors set out in **section 13(1)** can apply when several requests are made at the same time, even though no single request would present such difficulties. This provision applies to any time limit extension, even if only an additional 30 days is required.

The public body should reference the factors outlined in **section 13(1)** when requesting an extension from the Commissioner. If the Commissioner refuses to grant a time limit extension under **section 13(2),** the public body may consider each request separately to determine whether an extension is needed.

When the Commissioner refuses to grant permission for an extension under **section 13(1)** or **(2)**, the public body has a maximum of only 60 days to process the request.

Public bodies must continue to process a request while awaiting the Commissioner's response to an extension request.

***Documentation*:** Public bodies must document the reasons for a time limit extension. This is required to support the public body's decision to extend, for a request to the Commissioner for an extension of more than 30 days, and in case of a complaint by the applicant to the Commissioner.

Notification**: Section 13(4)** of the *Act* requires a public body to notify the applicant that an extension is being taken, the reason for it, the date when a response can be expected, and that the applicant has the right to make a complaint to the Commissioner about the extension.

Model Letter D in Appendix 3 deals with time extensions. This notice is required as soon as it is apparent that the request cannot be processed within the initial 30-day time period.

When a request for extension is made to the Commissioner, the notice should be sent to the applicant before the Commissioner's final decision has been made as to whether or not the extension will be granted.

If an applicant complains to the Commissioner about an extension, the public body continues to process the request throughout the review period.

After investigating a complaint about a time limit extension, the Commissioner may either confirm or reduce the extension as provided in **section 68(3)(b)**.

Conditions affecting response times:

- *Third party notice*: When a public body gives notice to a third party under **section 29**, the deadline for a final response to an applicant must take into account the time required to allow the third party to respond. No decision may be made before *either* 21 days after the day notice is given *or* the day a response is received from the third party, whichever is earlier. The public body should notify the third party as soon as possible after receiving a request in order to minimize the delay in responding.

Giving a third party notice is discussed in Chapter 5 of this publication.

- *Transfer of request*: Where a public body decides to transfer a request to another public body, the *Act* requires it to do so within 15 days of receiving the request. The second public body then has 30 days after receiving the request to respond, unless it seeks an extension on one of the grounds set out in **section 13**.

Day of response**:** The Alberta *Interpretation Act* provides that, if the day a response is due falls on a statutory holiday or a day when the office of a public body required to respond is closed, then the response is due on the next business day.

The head of the public body is responsible for determining whether the office that is authorized to handle requests is closed. For example, a school board is still responsible for processing requests when offices of the administration are open but individual schools are closed. A process must be established in such cases to ensure records are retrieved.

If a public body such as a small municipality completely closes its office for staff vacations, then the completion of the request will be affected and can legitimately be delayed until the first working day after the office reopens.

3.4 PROCESSING A FOIP REQUEST

Overview

In responding to FOIP requests, it is important that a public body clearly assign responsibilities for the various processing steps. This section outlines the assignment process and describes the responsibilities of program areas in a decentralized organizational model, where retrieval and review of records is performed in program areas and the office of the FOIP Coordinator carries out management of the final decision-making. In a centralized model, the office of the FOIP Coordinator will carry out all the duties outlined in this chapter.

Public bodies should develop procedures to govern the processing of requests and to ensure that processing occurs within established time limits and in accordance with the requirements of the *Act*. Public bodies should also create and retain documentation on their processing of requests. The forms provided in Appendix 6 of this publication may be used or adapted for this purpose.

Before beginning to process a request, the FOIP Coordinator should determine whether the request can be handled outside the *Act*. If so, and if no other fee structure is in place, the initial fee should be returned to the applicant along with a copy of the records. If there is a procedure in place to refer an applicant to the appropriate program area, the fee should not be returned until the applicant has agreed to have the request handled outside the *Act* by the program area.

The applicant must agree to withdraw the request; otherwise, the public body is required to respond to it in accordance with the requirements of the *Act*.

Model **FOIP Request Charts** are provided in Appendix 5.

Initial Control

Once a request is received in the office of the FOIP Coordinator, it should be registered and logged (this is done electronically if an automated tracking system is in use).

It should then be placed in a request file and details of the request forwarded to any program area that has custody or control of requested records. The office of the FOIP Coordinator can record this assignment of responsibility on the request tracking system.

The request should be accompanied by a **FOIP Transmittal Memorandum** and **Access Request Review Form** for recording all activities and the time involved in processing the request, in order to document these activities and assess the appropriate fees. A model **FOIP Transmittal Memorandum** and an example of an **Access Request Review Form** are included in Appendix 6 of this publication.

The identity of the applicant should be disclosed only:

- to those officials and employees of the public body who have a need to know it in order to carry out their job duties; and

- to the extent necessary to carry out the public body's functions in processing the applicant's request.

For instance, where the request is for general records, the FOIP Coordinator should forward only the request for records and not the name and other identifiers of the applicant to program areas within the public body (see *IPC Investigation Report 98-009*).

Locating Records

The program area is normally responsible for locating and retrieving all records relevant to a request under its custody or control, including those records that may reside in individual employees' offices, vehicles or homes, or in filing systems in storage areas. When applicable, records in the possession of contracted agencies may have to be located.

The program area should draw on the support of records or information management staff in providing the indexes and guides to appropriate records, where these are available, and to locate records.

Speed and accuracy are essential in identifying, locating, retrieving and, where appropriate, copying records pertinent to a request (where a request is for a large number of records, it may be appropriate that copies are not made immediately).

A rule of thumb for a basic, uncomplicated request involving the coordination of staff in different areas is that four working days are needed to pull together the working program file, with the pertinent records that need to be reviewed.

Scope of search: The *Act* applies to *all* records, as defined in the legislation, including electronic records, in the custody or under the control of the public body. All types of records responsive to the request, including electronic records, must be located and retrieved.

In addition, all areas where records are held – central active files, working files in individual offices, electronic repositories and off-site storage areas – must be searched, and staff requested to produce relevant records, as dictated by the nature and subject of the request.

Any records in the possession of contracted agencies and under the control of the public body will have to be located, copied, if appropriate, and transferred.

An applicant can ask the Information and Privacy Commissioner to review the adequacy of a search undertaken to locate records. When this happens, the public body will have to demonstrate that it made a reasonable search of all repositories where records relevant to the subject of the request might be located. See *IPC Order 96-022* for criteria the Commissioner uses in judging the adequacy of a search for records.

Conditions relating to the disposition of records: **Public bodies must not dispose of any records relating to a request after it is received, even if the records are scheduled for destruction under an**

approved records retention and disposition schedule.

This includes any e-mail and transitory records relevant to the request that may exist at the time the request is received. In effect, the receipt of a FOIP request freezes all disposition action relating to records covered by the request until the request has been completed and any appeal to the Commissioner decided.

For continuing requests, disposition action freezes at the point when the request is reactivated in accordance with the agreed schedule.

The file transmitting the request to the program area should include a reminder that it is an offence to destroy any record (**section 86(1)(e)**), or to alter, falsify or conceal any record, or to direct another person to do so (**section 86(1)(c.1)**) in order to evade a request for access to records. These offences are punishable by a fine of up to $10,000.

Where records have been destroyed prior to the receipt of a request, in accordance with an approved records retention and disposition schedule, the public body's response to the applicant should indicate that the records have been destroyed, quoting the authority for and date of destruction.

When records have been transferred to the Provincial Archives of Alberta or the archives of the public body, the request should be transferred to the archival authority for processing, unless some other arrangement between the two organizations exists (see *IPC Order 96-022*).

***Copying retrieved records*:** Once the records have been located, either the program area or the office of the FOIP Coordinator, as appropriate, prepares them for review and completes the request documentation.

This may involve the copying and numbering of all records pertinent to the request and preparing:

- a list of all records areas searched;
- a list of the records located in each records area, along with identifying data and parts of file lists, data dictionaries or other finding aids used in locating the records; and
- a log of staff time spent searching for and retrieving the records.

When there is a very large number of records involved, lists of the records rather than copies of them may be more appropriate.

Preliminary Assessment

There are a number of administrative matters that the FOIP Coordinator should consider very early in the request process, but after the program area has had an opportunity to consider the extent and nature of the request and to locate the records. This discussion will inform the preliminary review of the records, which will be done either by the FOIP Coordinator or, in larger organizations, by the office of the FOIP Coordinator in cooperation with the program contact and representatives knowledgeable about the subject matter and records involved.

Questions to ask at this stage are:

- Does it appear that all relevant records have been located and do they appear to satisfy the request?
- Are there any records referenced in the request or the located records that have not yet been located?
- Are any of the records excluded from the scope of the *Act* under **section 4** or subject to other legislation that prevails over the *FOIP Act*?
- Can the records, in whole or in part, be released immediately without line-by-line review?
- Should all or a portion of the request be transferred to another public body with greater interest in the records? See section 3.3 of this chapter, Response Time Limits, for legislative requirements and policies relating to the transfer of requests.
- Does it appear that records may be found in program areas other than those already identified, and should the search be widened?
- What is the extent and nature of consultation required with other program areas within the public body? Responsibility for ensuring that these consultations occur should be clearly assigned.
- What is the extent and nature of external consultation required with other public bodies and levels of government? Responsibility for conducting these consultations should also be clearly assigned.
- Do the records contain third party business information or personal information that may require third party notification?
- Will the time required to respond to the request likely exceed the 30-day time limit? Are there grounds for an extension of the time limit?
- Will fees in addition to the initial fee (if applicable) be assessed for the processing of the request?

From this preliminary review, the FOIP Coordinator may, depending on the level of delegation, either recommend or undertake actions related to:

- the transfer of all or part of the request;
- the immediate release of all or some of records;
- the extension of time limits;
- third party notification; or
- the assessment of fees.

Each of these activities involves a notice to the applicant. Notices are considered in this publication as follows:

- release of a record is discussed in section 3.5 of this chapter;
- extension of time limits is discussed in the section 3.3 of this chapter, Response Time Limits;
- third party notification is discussed in Chapter 5;
- transfer of requests is discussed in section 3.3 of this chapter; and
- fees are discussed in this section (3.4) below.

Notices

Various notices are required under the *Act*. Of particular importance are those provided:

- to inform an applicant of a fee estimate;
- to report to an applicant about the progress of a request (e.g., any extension of the time limit for responding);

- to notify a third party (a business or an individual) that information provided by the third party or personal information about the third party has been requested, and that an opportunity is being provided for comment as to whether or not the information should be disclosed; and
- to advise the applicant of the decision on the disclosure and provide information about access to the requested records if access is granted.

Section 78 of the *Act* provides that a notice or other document to be given to a person is to be given:

- by sending the notice or document by prepaid mail to the last known address of the person;
- by personal service;
- by substitutional service if authorized by the Commissioner; or
- by means of a machine or device that electronically transmits a copy of a document, picture, or other printed material by means of a telecommunications system.

The choice of how to give notice or send a document depends very much on the circumstances. Normal methods will be by mail and fax, since these are common, effective ways of communicating. There will be circumstances, however, when other methods may have to be used. This may be the case when addresses are uncertain, when the number of persons, organizations or groups to be contacted is large, or when there is a need to assure delivery to a specific person. Other methods of delivery may be more effective in these circumstances.

Personal service means a method of delivery whereby it can be shown that the person to be served actually received the document.

Substitutional service usually takes the form of a notice presented in the media. This may be a general notice, as often appears in newspapers and weekly journals, or a more specific notice (e.g., a third party notice to a large number of small companies) published in the leading trade magazines for the particular business sector concerned.

Public bodies should assess the circumstances requiring the notice and choose the most effective and economical approach.

The **Model Letters** in Appendix 3 provide examples and options for all the notices required under the *Act*.

Assessing Fees

An important principle underlying the *FOIP Act* is the use of fees to help offset the cost of providing applicants with access to records under the legislation.

The *Act* provides for a reasonable and fair fee structure that is intended to support effective provision of FOIP services.

Section 87 establishes that:

- a public body may require an applicant to pay fees for services as provided for in the FOIP Regulation (**section 87(1)**);
- for personal information, such fees shall be restricted to the cost of providing a copy of the information (**section 87(2)**);

- if fees are required under **section 87(1)**, an estimate of the total fee must be prepared by the public body for the applicant before providing the services (**section 87(3)**);
- the public body may excuse an applicant from paying all or part of a fee if, in the opinion of the head of the public body:
  - the applicant cannot afford the payment or for any other reason it is fair to excuse the payment; or
  - the record relates to a matter of public interest, including the environment or public health or safety (**section 87(4)**);
- the fees referred to in **section 87(1)** must not exceed the actual costs of the services provided.

Section 89(c) enables local public bodies to establish their own fee structures provided they follow **section 87** of the *Act* and do not exceed the fee structure set out in the FOIP Regulation. This is done through a by-law or, where applicable, other legal instrument by which the local public body acts.

GST is not charged on fees for processing FOIP requests.

General Records

Section 10 and **Schedule 2** of the FOIP Regulation set out the fees that may be charged for processing a general access request.

The head of a public body may require an applicant who makes a request under the *Act* to pay fees for the following services:

- locating and retrieving a record;
- producing a record from an electronic record;
- preparing a record for disclosure (to cover the time taken to physically sever the record);
- providing a copy of a record;
- creating a new record under **section 9** of the *Act*; and
- supervising the examination of an original record.

No fee may be assessed for time spent in reviewing a record to determine whether or not all or part of it should be disclosed.

If new records have to be created from an electronic record, the public body may use acceptable industry standards to ensure accuracy and completeness of the records, process the information according to its usual procedures, and charge for these services as a part of its fee (see *IPC Order 99-014*).

The fee provision is discretionary in nature, but normally fees will be assessed for all general requests under the *Act*. Fee waiver provisions are set out in **section 87(4)** of the *Act*. The FOIP Regulation sets out the schedule of maximum fees that may be charged. Public bodies may choose to charge less than these rates but not more.

A person who makes a request for access to a general record, which is not a record of the applicant's own personal information, is required to pay:

- an initial fee of $25.00 at the time that a one-time request is made; or
- an initial fee of $50.00 when a continuing request is made.

This initial fee covers the work involved in registering the request, locating and retrieving records, and in some instances providing access to records. For simple, straightforward requests involving a small volume of records, it will be the only fee paid. For complex requests or requests involving a large volume of records, the initial fee would probably not cover location and retrieval of all records, but would cover the preparation of a fee estimate.

No additional fees are charged unless the amount of fees required to process the request for general records, as calculated by the public body to which the request has been made, exceeds $150.00.

When the amount estimated exceeds $150.00, the total amount is charged to the applicant.

The maximum fees to be charged for services provided to applicants are set out in **Schedule 2** of the FOIP Regulation.

Processing of a FOIP request for general records must not commence until the initial fee has been paid.

Personal Information

Section 11 of the FOIP Regulation establishes fees to be charged to an individual for accessing his or her own personal information.

In the case of a request for an applicant's own personal information, an applicant will pay only copying fees, and then only when those fees exceed $10.00, as determined by the public body in accordance with the rates established in **Schedule 2** of the FOIP Regulation.

Subject to the fee waiver provision (**section 87(4)**), when the fee exceeds $10.00, the total amount will be charged to the applicant.

Fee Estimates

Section 12 of the FOIP Regulation governs the provision of fee estimates under the *Act*.

When an estimate is provided to an applicant in accordance with **section 87(3)** of the *Act*, the applicant will be provided with the following details:

- the time required and cost of locating and retrieving the record;
- the time required and cost of preparing the record for disclosure;
- the cost of copying the record;
- any computer time involved in locating and copying a record or re-programming to create a new record, as appropriate;
- supervision costs when an applicant wishes to examine the original record; and
- any costs for shipping records to another location for examination or for shipping copies of records directly to the applicant.

An estimate for access to a record of the personal information of the applicant would only include the cost of copying the record.

In the case of continuing requests, the estimate must include the total fees payable over the course of the continuing request (*see IPC Order 97-019*).

This detailed estimate is provided to the applicant as a part of a notice that includes:

- a request that at least 50% of the estimate be paid in advance of the request being processed, or in the case of continuing requests, a request that at least 50% of the estimate for the first instalment be paid in advance of the request being processed;
- a statement that the applicant has 20 days to inform the public body that the estimate is accepted and to pay the deposit; and
- a statement that the applicant has the right to ask the head of the public body to excuse all or part of the fee and may request a review by the Information and Privacy Commissioner if the fees are considered too high or otherwise inappropriate, or if a request for a fee waiver has not been granted.

Model Letter E in Appendix 3 may be used to provide this notice.

This information gives the applicant the basis on which to accept the charges or take other action. This might include narrowing the request, reviewing original records, which would incur supervision costs but would cut down on copying costs, seeking a fee waiver, or requesting review of the fees by the Commissioner under **section 62(1)** or **section 51(2).**

No further processing takes place until one of the following events occurs:

- a letter from the applicant agreeing to the charges and attaching payment of the deposit is received in the authorized office;
- written notification from the applicant modifying the request, and establishing a new basis for assessment of fees, is received in the authorized office;
- the public body agrees to a request for a fee waiver; or
- the Commissioner carries out a review and decides whether the fees are appropriate, or whether the head of the public body has appropriately exercised his or her discretion regarding a request for a waiver of fees, as applicable.

An applicant has up to 20 days to indicate whether or not the fee estimate is accepted. The applicant may choose to modify the request so as to change the amount of fees assessed. If no response has been received after 30 days, the public body may declare the request to be abandoned (see later in this section).

More detailed guidance on estimating fees is provided in *FOIP Bulletin No. 1, Fee Estimates*.

Fee estimates are not binding. However, a public body should do its best to estimate what the fees will be. The public body can revise its estimate in the course of processing the request, and may do so in cases where, for example, records are poorly organized.

If the estimate is too high, provision is made for making a refund to the applicant. If a fee estimate is too low, the public body has the discretion to request additional fees from an applicant. However, the fact that fees will be higher must be addressed with

an applicant as soon as it becomes apparent and not be left to the end of the processing period.

Deposits and Payment of Fees

Processing of a request ceases once a notice of estimate has been forwarded to an applicant and recommences immediately upon:

- receipt of an agreement to pay the fee; and
- receipt of at least 50% of any estimated fee that exceeds $150.00. (FOIP Regulation, **section 13(1)(a)**) or, in the case of a continuing request, receipt of at least 50% of the portion of the estimate applicable to the delivery of the instalment of the request to be processed (FOIP Regulation, **section 13(1)(b)**).

The balance of any fee owing is payable at the time the records are provided to the applicant (FOIP Regulation, **section 13(2)**).

If the amount paid is higher than the actual fees required to be paid, the balance paid will be refunded. The initial fee is not refunded (FOIP Regulation, **section 13(3)**).

The applicant should not be provided with access to a record until all fees owing for the processing of the request have been paid (section 6(3) of the *Act*).

Local public bodies should arrange for fees paid under the *Act* to be handled in the same way as other revenue.

Provincial public bodies that are funded by the provincial General Revenue Fund must process fees in accordance with directions from Alberta Treasury and deposit FOIP revenue into the fund designated by the Office of Budget and Management, Treasury (IMAGIS Account Code 446425).

Waiving Fees

Section 87(4) provides that a public body may excuse the applicant from paying all or part of a fee if, in the opinion of the public body:

- the applicant cannot afford the payment or for any other reason it is fair to excuse payment; or
- the record relates to the matter of public interest, including the environment or public health or safety.

Normally, an applicant will take the initiative in requesting a fee waiver, usually at the time of submitting the request itself. A public body must consider the request for a fee waiver from an applicant at the time it is made. If a request for waiver is part of the FOIP request, the public body will consider it when it is preparing a fee estimate and decide whether or not the request meets any of the waiver criteria and, if it does, whether or not a waiver is merited.

The public body does not need to waive all fees if it decides to grant a request to excuse payment. It can consider reducing the fee by a part of its total or not charging for certain services.

If an applicant has requested a fee waiver, and the public body does not grant it, the public body must notify the applicant that he or she may ask the Commissioner for a review of this decision (**section 87(4.1)**).

The Commissioner may conduct a review of the decision by the head of the public body under **section 62(1).**

Section 87(4) establishes the criteria for excusing payment of all or part of a fee.

***Applicant cannot afford to pay*:** In very limited circumstances, applicants may be indigent or living on social benefits but require information to assist them in exercising individual or group rights.

This type of situation arises most frequently with requests from individuals for information about themselves. Normally, applicants will state in a request why they are seeking a waiver. If they do not or if more information is required, the office of the FOIP Coordinator should phone the applicant and seek the information needed to make a decision.

Applicants should not have to undergo a wealth test to qualify for this type of waiver, but basic information on income and situation should be sought to satisfy the public body that an applicant may fall into this category. For instance, applicants may be asked to show evidence that they would suffer hardship if they were obliged to pay the required fee, including general information about their sources of income.

***Other reasons why it is fair to excuse payment*:** This is a general provision to cover situations where a public body may wish to excuse or reduce fees but has no specific authority to do so.

Examples of situations where it might be fair to excuse payment are:

- where an individual seeking his or her own personal information can show that the information is vital to the exercise of his or her rights;
- where the information is of general interest to several applicants and the records are being released to them more or less simultaneously. The first applicant should not bear the total processing costs for all the others and fees may be reduced accordingly.

***A matter of public interest, including the environment, public health or safety*:** This category of fee waiver generally covers situations where there is a public interest in disclosing all or part of a record.

This occurs when the information is likely to contribute significantly to public understanding of the operations or activities of the public body or is of major interest to the public in terms of environmental protection or protection of public health or public safety.

The Information and Privacy Commissioner has listed thirteen considerations which may be taken into account when considering a fee waiver in the public interest in *IPC Order 96-002* and *IPC Order 97-001*.

The criteria do not constitute a test, but rather set out points or questions that may help public bodies in considering waivers in the public interest.

These criteria are governed by two overriding statutory principles that must be taken into account on a general basis when dealing with both FOIP fees and fee waivers:

- the *Act* is intended to foster open and transparent government, subject to the limits contained in the legislation; and
- the *Act* contains the principle that the user should pay.

The Commissioner's questions relating to a waiver in the public interest are:

- Is the applicant motivated by commercial or other private interests?
- Will members of the public, other than the applicant, benefit from disclosure?
- Will the records contribute to the public understanding of an issue (that is, will they contribute to open and transparent public administration)?
- Will the disclosure add to public research on the operation of the public body or its responsibilities?
- Has access been given to similar records at no cost?
- Have there been persistent efforts by the applicant or others to obtain the records?
- Would the records contribute to debate on issues of public interest or to their resolution?
- Would the records be useful in clarifying public understanding of issues that fall within the mandate of the public body?
- Do the records relate to a conflict between the applicant and the public body?
- Should the public body have anticipated the need of the public to have the record?
- How responsive has the public body been to the applicant's request? For example, were some records made available at no cost or did the public body help the applicant narrow the request so as to reduce costs?
- Would the waiver of the fee shift an unreasonable burden of the cost from the applicant to the public body, such that there would be significant interference with the operations of the public body?
- What is the probability that the applicant will disseminate the contents of the record?

Public bodies should consider these questions when exercising their discretion whether or not to waive or reduce fees. A public body may ask an applicant requesting a fee waiver in the public interest to provide information relating to any of the points that appear relevant to the records under consideration.

If the Commissioner conducts a review of a decision not to grant a fee waiver in the public interest, the public body may find it helpful to show that it applied these criteria in making its assessment.

Fee waivers are discussed in more detail in *FOIP Bulletin No. 2, Fee Waivers.*

Abandonment of Requests

Often, it is clear when an applicant has decided not to pursue a FOIP request. Applicants will indicate either in writing or on the telephone an intention not to proceed with the request. This may be for a variety of reasons – for example, they have found that the information is available to them outside the FOIP process or they no longer need the information.

Sometimes, situations will arise where an applicant simply ceases to respond during the processing of a FOIP request. No indication is given that the applicant has decided not to pursue the request. He or she simply does not respond to queries from the public body.

When this latter situation occurs, **section 7.1** of the *Act* sets out provisions for declaring a request to be abandoned. The public body must have contacted the applicant in writing, and either sought further information that is necessary to process the request, or requested payment of or agreement to a fee.

If the applicant does not respond within 30 days of being contacted, the public body can advise the applicant, again in writing, that the request has been declared abandoned. A specific date for this declaration should be included in the notice. This notice must state that the applicant can ask for a review by the Commissioner of the decision.

In most cases, abandonment of a request occurs before processing of the request is completed. However, in some cases, an applicant abandons a request after processing is completed.

If the public body

- has responded to the applicant's request, stating where, when and how access will be given; and
- has requested that the applicant contact the public body about viewing the records;

and the applicant does not respond within 30 days, then the public body can advise the applicant that the request has been declared abandoned. The procedure outlined above will apply to such requests. It is good practice for a public body to keep the file active for a further 60 days in order to allow time for the applicant to request a review by the Commissioner.

Model Letter E(1) in Appendix 3 deals with this type of situation.

Line-by-Line Review of Records

Once the preliminary assessment has been completed, the various administrative matters have been sorted out and any necessary consultations are under way, a knowledgeable officer from the program area or, in centralized systems, the office of the FOIP Coordinator, will need to review the documents line by line.

A line-by-line review is essential to comply with the principle of severability set out in **section 6(2)** of the *Act*. This provision grants an applicant a right of access to any record from which excepted material can be reasonably severed.

Chapter 4 of this publication deals with the guidelines for the application of the exceptions to the right of access.
The reviewer offers a perspective on any harm that may result from release of particular information and identifies factors to be taken into consideration when exercising discretion to release or refuse access to the information. During a line-by-line review, the office of the FOIP Coordinator may identify

additional requirements with respect to third party notices or consultations.

***Documentation*:** During the line-by-line review, the person who reviews the records should document exceptions to be invoked, actions to be taken, reasons for each decision, and recommendations for responding to the request.

A model **Access Request Review Form** is provided in Appendix 6 of this publication. Public bodies may adapt this form for their internal use. This form will provide a detailed record of the results of the review and recommendations on the application of exceptions.

Thorough documentation at this stage ensures that the public body has the information required to assess recommendations from the program area and to formulate final decisions relatively quickly. It minimizes duplication of effort and ensures that the public body is in a position to explain decisions both to the applicant and to the Commissioner's Office, if there is a request for a review.

***Reviewer's recommendations*:** The person who reviews the records generally should prepare a summary of recommendations that identifies:

- information recommended for release;
- specific records or parts of records that are excluded from the scope of the *Act*;
- specific records or parts of records to which mandatory or discretionary exceptions to disclosure apply, with the reviewer's recommendations and reasons with respect to the discretionary exceptions (for guidance on the exercise of discretion, see Chapter 4 of this publication); and
- other general factors that may be pertinent in reaching a decision on a response to the request.

This report forms the basis for a discussion between the office of the FOIP Coordinator and the program area of recommendations for a draft final report on the response.

At this stage any legal advice needed to resolve issues arising from the request should be sought. Similarly, any interpretative or policy issues which need to be raised should be identified and consultation undertaken.

The draft final report should contain:

- a log of staff time spent locating, retrieving, copying and reviewing the records;
- a summary of file systems, offices and records storage facilities searched;
- copies of records covered by the request (where this is possible and appropriate given the volume of records or the fact that the applicant wishes to view the original records);
- documentation of the line-by-line review, identifying the specific information in the retrieved records that it is proposed to except from access;
- a summary of third party notices sent and responses received;
- a summary of results of consultations with other public bodies and levels of government; and
- a written summary of recommendations for release or

refusal, including brief background information to explain decisions.

The **Access Review Recommendation/ Summary** serves as the authority to produce the response to the applicant and should be signed by the official delegated to make this decision on behalf of the public body.

Creating a New Record

Under **section 9(2)** of the *Act* a public body has the obligation to create a new record from an existing electronic record if:

- the record is in the custody or under the control of the public body;
- the new record can be created using the public body's normal computer hardware and software and technical expertise; and
- creating the record would not unreasonably interfere with the operations of the public body.

The creation of a new record is part of the public body's duty to assist the applicant in locating the information that is the most useful and responsive to his or her request. The creation of a new record from data that can be manipulated may be an advantage to public bodies in some instances.

Excepted material can sometimes be easily suppressed, saving long and tedious severing procedures. The applicant is also often very satisfied with the information he or she receives because it is in a more usable or understandable form. This provision is one to consider when dealing with requests involving electronic data and information.

This is the only case where the legislation requires a public body to create a new record.

Care should be taken to explain the methods used and what information is being suppressed so that the applicant does not think that information is being manipulated to alter the record or place a different perspective on it. Public bodies should also take reasonable steps to ensure the information is accurate (see *IPC Order 99-014*).

This provision is mandatory but extends only to situations where the record can be created using the normal hardware, software and technical resources of the public body, and when creating the record would not unreasonably interfere with the operations of the public body.

The office of the FOIP Coordinator should consult with both the program and information technology areas to assess the time and resources that would be required to create the record and the impact that this use of resources would have on its day-to-day activities.

A public body may also decide to create a record, even when there is no requirement to do so, if an applicant requests information to which a discretionary exception applies and the public body is willing to disclose the requested information but not the record containing the information.

Responsive Information

Records that have been identified as responsive to a request in an initial search may include information that is not responsive. Careful examination of the request is required to ensure that the reply is complete but also that information that is non-responsive to the request is removed.

The fact that an applicant already has or knows the substance of the information, or has knowledge of the contents of the record, does not mean that the record can be considered non-responsive. The public body's obligation is to address the applicant's entire request (see *IPC Order 98-005*). However, a public body and an applicant may agree not to make copies of records available in order to save costs.

Removal of non-responsive information must occur before severing takes place using the exceptions in the *Act* (see *IPC Order 97-020*).

This process applies only when an applicant requests specific *information*, such as his or her own personal information. If an applicant asks for a *record*, then the whole record is generally considered responsive and any part of the record that is not to be disclosed must be severed on the basis of the exceptions in the *Act* (see *IPC Order 99-002*). Despite this general rule, the public body may treat portions of a record as non-responsive if they are clearly separate and distinct and entirely unrelated to the access request (see *IPC Order 99-020*).

Certain records that are identified as responsive to a request may be records that are excluded from the scope of the *Act* under **section 4**. If a public body chooses to provide access to excluded records, it should be made clear to the applicant that the records are outside the scope of the *Act*. For information responding to a request involving excluded records, see section 3.5 of this chapter.

Severing Information

Many records contain both information that can be released and other information that should be excepted from disclosure. When information that falls within an exception can reasonably be severed from a record, an applicant has a right of access to the remainder of the record (**section 6(1)**).

When a discretionary exception applies, a public body must use discretion not only in applying the exception, but also in determining how much of the information is severed. This is the reason for undertaking a line-by-line review of a record. The object of severing is the use of discretion to release as much information as possible, without causing the harm contemplated by the exception.

The only exception to this procedure is when using the exception for legal privilege. When legal privilege applies to a record, the whole record is excepted.

Scope: Severing applies to all records regardless of format or previous actions taken. The fact that an applicant may already have obtained copies of some of the records in other ways does not preclude severing to respond to a request (see *IPC Order 98-016*).

When severing is required for information stored on specialized media, technical expertise should be sought as to the best way to excise information while recording that severing has been done and for what reason.

In some rare cases a record cannot be severed. The public body then refuses access to the whole record and must be prepared to demonstrate to the Information and Privacy Commissioner the technical reasons underlying the inability to sever. Examples include personal information of two or more individuals so intertwined in a record that severing would be extremely difficult and time-consuming, or when, after severing, the severed record would make no sense (see *IPC Order 96-019*).

Procedures: During the line-by-line review of records pertinent to a request, the reviewer should mark up copies of paper-based records and keep notes about information in other media that may qualify for an exception. The review and severing of records may require a significant amount of time. The review procedure should ensure that all records responsive to the request are reviewed.

The objective in severing is to remove from the body of a record only the information that meets the conditions for an exception. The *Act* requires that all information in a record that is responsive to the request and which will be intelligible to the applicant after severing be disclosed.

The process is governed by reasonableness, and the public body exercises discretion in determining whether or not discrete portions of information contribute to the overall understanding of the subject matter at issue.

Employees should be encouraged to draft documents with information that the public body may wish to except, such as recommendations and advice or personal data, segregated in particular parts of the document. This will make the severing process more efficient for current documents.

Part of the final decision as to what information will be released and what information will be refused is also a decision on the extent to which the severing process will be applied. Once that decision is taken, the office of the FOIP Coordinator can use several methods of severing:

- use of non-permanent white tape over the excepted portion of a copy of the record and recopying to obtain the record to be released;
- use of liquid eraser over the excepted portion of a copy of the record and recopying to obtain the record to be released; or
- use of a photocopying machine with editing features suitable for severing.

Whatever method of severing is selected, the office of the FOIP Coordinator must ensure that none of the excepted information remains visible. For this reason, the use of markers is not recommended.

Indication of severing: Regardless of the severing method, a public body must indicate the section number of any exception used to sever information, either in the space left after the severing or in the margin closest to the severed information. Where one or more entire pages have been removed, the number of pages severed must be indicated, along with an explanation of the applicable exception(s) used to sever the information.

In cases where a single page or a continuous sequence of pages has been totally severed, the exception(s) applied and the pages to which they applied should be listed in the response letter or collated on a single page. It is neither necessary nor helpful to provide applicants with multiple blank pages.

In some cases, particularly with law enforcement records, placing the relevant section in the space of the severed information may itself reveal or imply information that could cause harm. The inclusion of the reason for an exception with the remainder of the record could result in an indirect form of information disclosure. In these circumstances, it is permissible for the public body to omit section numbers on the severed pages and list the relevant sections supporting severance in the letter of notification.

Indicating why information was severed from records helps an applicant understand why part of the information requested has been refused and permits an independent review of the decisions taken by the public body. See *IPC Practice Note No. 2, Informing the Applicant of Grounds for Refusal.*

Maintenance of Copies

A public body should keep a file for each request processed. This file should include an unmarked copy of the records gathered in response to a request and a copy of the severed documents released to the applicant.

This practice helps support the public body in any review by the Information and Privacy Commissioner, and in making decisions regarding requests for the same or similar records in the future. Maintaining copies can simplify the process of responding to the same or a similar request. However, unless the new request is made shortly after the original, there is still a need to review the records again (see *IPC Order 99-021*). The passage of time and any changes in the context surrounding the records may result in more information being released. The rule is that each FOIP request needs to be processed as a separate request and decisions need to be made in relation to the particular circumstances that apply at the time of the request.

This does not mean that every request is unique. There are similar types of requests that lend themselves to categorization and simple release mechanisms. Often it is possible to create easily severed documentation that is released routinely. This might be done either because the information is in high demand or because disclosure of the information supports overall accountability for a program or activity. In some cases, active dissemination may also be warranted.

3.5 RESPONDING TO A FOIP REQUEST

Overview

Section 11(1) of the *Act* provides that an applicant must be told:

- whether access to the requested record or part of it is granted or refused;
- if access is to be granted to the record or part of it, where, when and how access will be given; and

- if access is to be refused, the reason for refusal and the provision of the *Act* on which this is based, the name and location of an employee who can explain the reasons for the refusal, and that the applicant may ask for a review of that decision by the Information and Privacy Commissioner.

When providing an applicant with access to his or her own personal information, a public body must be satisfied that the individual receiving the information is, indeed, the individual the information is about or a duly appointed representative of that person.

For information on appointment of representatives see Chapter 7.13 of this publication.

Identification can usually be confirmed from the context of the request process, but, where there is doubt or the information is sensitive, the public body should request normal identification (e.g., a birth certificate or driver's licence) before providing the information.

Fees

In responding to applicants, public bodies must collect all outstanding fees before releasing the records to the applicant.

See Chapter 3.4 of this publication for information on assessment of fees.

Model Responses

The applicant must be provided with a response to a request. **Model Letters G, H, I, and J** in Appendix 3 provide guidance and options for drafting the various types of final responses to FOIP requests.

In all cases when access is denied, where the record is excluded from the *Act*, or where the public body refuses to confirm or deny the existence of a record, the response letter must state that, if the applicant requests a review of the decision by the Information and Privacy Commissioner, he or she should provide the Commissioner with

- the request number assigned by the public body,
- a copy of the decision letter, and
- a copy of the original request when requesting a review.

Generally, the response letter should address the outcomes of the search and review of records in response to a request.

***Record does not exist*:** The public body cannot locate records responsive to the request. If, after consulting with the applicant, it still appears that no records exist, a letter should be sent informing the applicant of that fact and of the steps taken to attempt to find records. Where a record has been destroyed prior to receipt of the request, information should be provided on the date of destruction and the authority for carrying it out (e.g., the appropriate records disposition number or authorization).

***Access is provided*:** There is a determination that access will be provided because the information falls within the scope of the *Act*, and the information does not qualify for any exception, or it qualifies for a discretionary exception but the public body has used its discretion in favour of releasing the information.

Some requests will involve records that take little time to review or are easily releasable. In these instances, the public body should release available records as soon as possible rather than waiting until all records are ready for disclosure. This is often possible when some records are ready for release and other records have been sent to third parties for consultation.

The applicant will have indicated, in accordance with **section 7(3)** of the *Act*, whether he or she wishes a copy of the record or to examine the original record. If the request is for a copy and it can be reasonably reproduced, **section 12(2)** of the *Act* requires that the copy be included in the package. This will be done only if the balance of the fees has been paid.

If it is not possible to include the records, the same provision requires that the applicant be given the reason for the delay and told where, when and how the copy will be provided. Delay at this stage is unusual, except where there is a requirement to pay any outstanding fees before access is provided.

In some instances, the applicant may have asked to examine a record but the record cannot be reasonably severed for examination, or the record is in a format that does not readily lend itself to examination (e.g., a microfilm with much excepted material on it). In these instances, the public body may choose to provide a copy of the record to the applicant.

Section 3 of the FOIP Regulation covers the two types of situations described above.

***Excluded records*:** In some instances all or some of the records may be excluded from the scope of the *Act* under **section 4**. Where this is the case, the applicant is informed that the record or information is excluded from the application of the *Act*. The letter should cite the specific exclusion in **section 4** that applies, and state that the applicant has the right to ask the Information and Privacy Commissioner to review the decision of the public body that the specified exclusion in **section 4** of the *Act* applies.

It may occur that a record responsive to a request is excluded from the application of the *Act*, but the public body is considering providing access to it outside the *Act*. In such cases, public bodies should consult with any affected parties. For example, if the record was created by or for an Officer of the Legislature or an MLA, the Officer of the Legislature or the MLA concerned should be consulted.

In instances where access is provided to an excluded record, it is important that the letter of response inform the applicant that the record is excluded, citing the provision of **section 4** that applies, but indicating that the public body has chosen to provide access to the record outside the *Act*.

***Access denied*:** Access is denied to all or part of a record if the information falls within a mandatory exception; the information falls within a discretionary exception and the decision is to deny access; or the information lies outside the scope of the *Act*. In these instances, the response provides:

- the reasons for refusal and the sections (i.e., the specific subsections and paragraphs) on which the refusal is based;
- the name, title, business address and business telephone number of the FOIP Coordinator or other official who will answer any questions the applicant may have; and
- a statement that the applicant has the right to request a review of the decision under **section 62(1)** of the *Act* and that this request must be made within 60 days after notification of the decision.

***Refusal to confirm or deny existence of record*:** In some circumstances, the knowledge that a record exists may cause harm to a law enforcement matter (**section 19**), may pose a danger to an individual's or the public's safety (**section 17**) or may invade the personal privacy of a third party (**section 16**). **Section 11(2)** of the *Act* permits a public body to refuse to confirm or deny the existence of a record in these instances (see *IPC Order 98-009*).

Copies of Requests and Records

When a public body has responded to the applicant, the FOIP Coordinator should ensure that the central request file is complete and includes:

- all internal and external correspondence;
- copies of records reviewed;
- copies of all records that were released to the applicant, either severed or complete; and
- any other information documenting the request management process.

Closure and Retention of Request Files

It is good practice to keep a request file active for 60 days after responding to a request in order to allow time for a request for a review by the Commissioner. If a review is requested, the file will be reopened and remain open until the review process is complete.

Once the file is closed, either because the public body has responded to the request, or a review has been completed, the public body must retain the file for at least one year to meet the retention requirements of **section 34(b)** of the *Act*.

In addition to meeting the requirements of the *FOIP Act*, a provincial public body is also obliged to comply with its records retention and disposition schedule. For provincial public bodies, this may be the Administrative Records Disposition Authority (ARDA), produced by Alberta Innovation and Science, Records and Information Services, or it may be another schedule approved by the Alberta Records Management Committee (ARMC).

Local public bodies must not transfer, store or destroy request records except in accordance with the by-law, resolution or other legal instrument by which the local public body acts, or, if no such instrument exists, except as authorized by the governing body of the local public body (**section 3(e)**).

Chapter 4
Exceptions to the Right of Access

4.1 OVERVIEW

Section 2(a) of the *FOIP Act* allows any person a right of access to records in the custody or under the control of a public body. **Section 2(c)** allows individuals a right of access to personal information about themselves that is in the custody or under the control of a public body.

Both rights are subject to limited and specific exceptions where release of information would result in disclosure of a particular category of information or would be harmful to a public or private interest. These exceptions are set out in **sections 15** to **28** of the *Act*.

In addition, **section 5** of the *Act* stipulates that when another Act of Alberta or a regulation under the *FOIP Act* expressly provides that the other Act prevails, the provisions of that Act apply, not those of the *FOIP Act*. In some circumstances, this will prevent disclosure of information. This provision is explained in section 4.2 of this chapter.

This chapter explains the various exceptions which require or allow a public body to refuse to disclose information to an applicant who makes a request under the *Act*.

It is important to remember that a basic principle of the *FOIP Act* is to give the public access to the records of a public body. Any exceptions to the right of access should be applied in a limited and specific way to provide as much access to information as possible.

Generally, an applicant has a right of access to all or part of any record that is the subject of the request. Refusal to disclose all or part of a record will occur only where the *Act* provides a specific exception to releasing all or part of a record.

A record cannot be withheld simply because its title or nature indicates that it may contain sensitive information. As well, access cannot be denied because disclosure may embarrass a public body or expose it to liability.

Each record must be carefully reviewed, in consultation with program staff knowledgeable about the subject, to determine whether it may be disclosed or whether an exception in the *Act* applies.

Public bodies should interpret the exception provisions narrowly. Only the specific information that is excepted from disclosure will be withheld.
The exceptions in the *Act* provide the only basis for refusing to disclose information, and public bodies are required to release information unless the *Act* expressly provides that all or some of the information in a particular record may be excepted from disclosure.

More than one exception may apply to all or part of a record. A public body should take into account all relevant factors when considering whether an exception to an applicant's right of access applies to a record.

No further exceptions can be applied once the Commissioner has made a decision on those that have been applied. However, the Commissioner will apply any mandatory exceptions that have not been applied by the public body (see *IPC Order 98-020*).

The exceptions may apply to requests for general information and also to requests from an individual for his or her own personal information.

The majority of requests for review to the Information and Privacy Commissioner under **section 62** of the *Act* will arise from refusal to provide access. Public bodies should be prepared to document and defend their decisions not to disclose particular information.

Mandatory and Discretionary Exceptions

There are two types of exceptions under the *Act* – mandatory exceptions and discretionary exceptions.

***Mandatory exceptions*:** Mandatory exceptions commence with the phrase "the head of a public body must refuse to disclose."

If information falls within a mandatory exception, a public body must refuse to disclose all or part of the record as required.

The only case where a mandatory exception may not apply is where there is a public interest that overrides it as provided in **section 31** of the *Act*. See Chapter 6 of this publication.

The legislation recognizes that certain kinds of information should not be disclosed and provides mandatory exceptions to protect that information.

Mandatory exceptions apply to information if:

- disclosure would be harmful to the business interests of a third party (**section 15(1)**);
- the information is about a third party and is in a tax record (**section 15(2)**);
- disclosure would be an unreasonable invasion of personal privacy (**section 16**);
- the information is in a law enforcement record and its disclosure would be an offence under an Act of Canada (**section 19(3)**);
- the information would reveal Cabinet or Treasury Board confidences (**section 21**);
- the information is subject to legal privilege and relates to a person other than a public body (**section 26(2)**); and
- disclosure is prohibited by another Act of Alberta or a regulation under the *FOIP Act* (**section 5**).

***Discretionary exceptions*:** Discretionary exceptions to the right of access permit a public body to choose whether or not to withhold all or part of a record.

Discretionary exceptions commence with the phrase "the head of a public body may refuse to disclose." There are eleven discretionary exceptions:

- disclosure harmful to individual or public safety (**section 17**);
- confidential evaluations (**section 18**);

- disclosure harmful to law enforcement (**section 19(1)** and **(2)**);
- disclosure harmful to intergovernmental relations (**section 20**);
- local public body confidences (**section 22**);
- advice from officials (**section 23**);
- disclosure harmful to the economic or other interests of a public body (**section 24**);
- testing and audit procedures (**section 25**);
- legal and other privileged information of a public body (**section 26**);
- disclosure harmful to the conservation of heritage sites, etc. (**section 27**); and
- information that is or will be available to the public (**section 28**).

Discretionary exceptions require two decisions by a public body:

- a factual determination must be made as to whether information falls within the category of information that may be withheld from disclosure; and
- the head of the public body must exercise his or her discretion as to whether information should be withheld.

Harm

Some discretionary exceptions are based on a harms test. This generally provides that access to all or part of a record may be refused if disclosure could reasonably be expected to harm a particular public or private interest.

Harm is defined as "damage" or "detriment" and each exception is designed to prevent the occurrence of particular "harms." These are discussed in detail in the individual sections of this chapter dealing with the exceptions.

A number of considerations are involved in making a judgment as to harm, but three general factors should be taken into account by public bodies in making such decisions. These are the degree to which the harm is specific, current and probable.

Specific: Is it possible to identify the detrimental effect on the interest or actual party that will suffer harm? To qualify, the injury cannot be a vague general harm.

Current: Is it possible to identify the detrimental effect at the time the exception is claimed or in the foreseeable future? Records which have been protected from disclosure in the past should be reassessed when a new request is received to ensure that the previously identified harm is still a factor.

Probable: Is there a reasonable likelihood of the harm occurring?

For a detailed discussion of the concept of harm see *IPC Practice Note No. 1, Applying "Harms" Tests*.

Other Discretionary Exceptions

In a few discretionary exceptions, the basis of the exception is that disclosure would reveal a certain class of information, such as advice from officials or the substance of *in camera* meetings. In such cases there is no need to address the harm that the disclosure may cause, although this may be a factor in exercising discretion.

Exercise of Discretion

The exercise of discretion is fundamental to applying the *Act*. The *Act* is based on the principle that the public has a right of access to information in the custody or under the control of public bodies. Subject to limited and specific exceptions, information should not be withheld unless there is an overriding harm or another sound reason for non-disclosure identified in one of the *Act*'s exceptions.

A discretionary exception requires a public body to determine whether harm is likely to result from the release of information that falls within the exception or, if the exception does not have a harms test, whether the interest outlined in the exception should be protected. If no harm is apparent or the particular interest is not adversely affected, the principle and spirit of the *Act* dictate that the public body should release the information.

The exercise of discretion requires the head, or staff member delegated to make such decisions, to weigh all factors, and consult with other public bodies if appropriate, in determining whether or not information that qualifies for a discretionary exception should be withheld.

The exercise of discretion is not a mere formality where there is a cursory examination before the appropriate authority denies access. The public body must be able to show that the records were reviewed, that all the relevant factors were considered and, if the decision is to withhold the information, that there are sound reasons to support the decision.

If there is a request for review, the Information and Privacy Commissioner decides whether or not an exception applies in a particular circumstance. If a discretionary exception has been properly applied, the Commissioner cannot overrule the head's decision. The Commissioner can, however, require the head to reconsider a decision if it appears that the obligation to exercise discretion has been disregarded, or where discretion has been exercised without due care and diligence or for an improper or irrelevant purpose (see *IPC Order 96-017*).

Once a public body has determined that all or part of a requested record falls within a discretionary exception, the public body must decide whether to release the information despite the existence of grounds for refusal. In making a decision, the public body must take into account all the relevant circumstances, as well as advice solicited from within the body, from other public bodies and from other affected parties.

A public body exercises discretion to withhold information on a request-by-request basis, with specific reference to the information requested and the particular circumstances of the case.

A public body must not replace the exercise of discretion with a blanket policy that information will not be released.

However, public bodies can develop guidelines to help guide the exercise of discretion, provided they are not interpreted as binding rules.

Some factors that should be taken into account when exercising discretion include:

- the general purposes of the *Act*; public bodies should make information available to the public, and individuals should have access to personal information about themselves;
- the wording of the discretionary exception and the interests which the exception attempts to balance;
- whether the applicant's request may be satisfied by severing the record and providing the applicant with as much information as is reasonably practicable;
- the historical practice of the public body with respect to the release of similar types of records;
- the nature of the record and the extent to which the record is significant or sensitive to the public body;
- whether the disclosure of the information will increase public confidence in the operation of the public body;
- the age of the record;
- whether there is a definite and compelling need to release the record; and
- whether Commissioner's orders have ruled that similar types of records or information should or should not be disclosed.

(See *IPC Order 96-017.)*

Whether an exception is mandatory or discretionary in nature, the public body must consider whether section 31 of the *Act*, disclosure in the public interest, requires release of the information. (See Chapter 6 of this publication.)

Application of Exceptions

There is a general process that should be followed in applying all exceptions. There are five basic steps.

Step 1: Preliminary Examination

Undertake a general review of the record(s) to determine which exceptions may apply and to gauge the complexity of the case and the notices that will be required as part of the process.

Step 2: Detailed Review

Review the record(s) line by line to consider more thoroughly the nature and extent of the exceptions involved. Identify information subject to mandatory exceptions, where a public body has no discretion to disclose information, and information to which no exception applies.

Step 3: Exercise of Discretion

Where discretion is permitted, undertake any necessary consultation and decide, with respect to information where exceptions apply, whether any or all of the information will be refused.

Step 4: Severing

Sever that part of the record(s) to which the public body has decided that it is necessary to refuse access. This will leave a record with a number of blank spaces annotated with references to the section(s) of the *Act* applied to sever the record, or, if a sequence of pages has been severed, with a single page listing the exceptions applied.

Step 5: Response to Applicant

Prepare a response to the applicant following the guidelines provided in Chapter 3 of this publication.

Many exceptions are complicated. Reference should be made to the detailed advice provided in this chapter on the application of each of the specific exceptions.

4.2 RELATIONSHIP TO OTHER ACTS

Paramountcy

Section 5(2) states that if a provision of the *FOIP Act* is inconsistent or conflicts with another enactment, the provision of the *FOIP Act* prevails unless:

- another Act, or
- a regulation under this *Act*,

expressly provides that the other Act or regulation, or a provision of it, prevails over the *FOIP Act*.

Section 5(2) provides for situations where two legislative enactments cannot stand together. Compliance with one law would involve breach of the other. When this happens, **section 5(2)** provides the means for resolving the conflict or inconsistency.

Acts and regulations, and sections of Acts and regulations, that prevail despite the *FOIP Act* and the various conditions that apply are partly set out in **sections 15, 16** and **17** of the FOIP Regulation.

For the most part, the FOIP Regulation stipulates which sections of the Acts and regulations prevail. The exception to this is the listing of certain health care legislation in **section 15(2)** of the Regulation. In some of these cases, entire Acts and regulations made under them prevail.

Several other Acts also have provisions that prevail despite the *FOIP Act* (e.g., the *Municipal Government Act*, sections 299 to 301).

When considering records that might be excepted under the paramountcy provision, a public body has to be sure that the record(s) being reviewed have a direct relationship to the provision that prevails (see *IPC Order 98-007*).

If the Commissioner finds that a provision of the *FOIP Act* is inconsistent or in conflict with another enactment, and the other enactment is one that prevails, he has no jurisdiction over the information with respect to that provision (see *IPC Order 99-034*).

Public bodies considering legislation or regulations that will have paramountcy, in whole or in part, over the *FOIP Act*, must consult with Information Management and Privacy, Alberta Municipal Affairs, during the consideration and drafting process.

Increasingly, any required paramountcy will be included in other Acts, rather than in the FOIP Regulation. Public bodies should be familiar with their governing legislation.

Copyright Act

Section 32.1 of the *Copyright Act* (Canada) states that disclosure of a record pursuant to the *Access to*

Information Act (Canada), or disclosure pursuant to any like Act of the legislature of a province, does not constitute an infringement of copyright.

Public bodies are not infringing copyright by disclosing copyright material in response to a FOIP request.

4.3 DISCLOSURE HARMFUL TO BUSINESS INTERESTS OF A THIRD PARTY

Overview

Section 15(1) creates a mandatory exception for information which, if disclosed, would reveal certain types of third party information supplied in confidence, and could also result in one or more specified harms.

The *Act* provides that the head of a public body must refuse to disclose to an applicant information:

- that would reveal:
  - trade secrets of a third party; or
  - commercial, financial, labour relations, scientific or technical information of a third party;
- that is supplied, explicitly or implicitly, in confidence, if its disclosure could
  - reasonably be expected to harm significantly the competitive position or interfere significantly with the negotiating position of the third party;
  - result in similar information no longer being supplied to the public body when it is in the public interest that similar information continue to be supplied;
  - result in undue financial loss or gain to any person or organization; or
  - reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

Section 15(1)(a) to (c) provides a three-part test. The information in question must:

- **be of a type set out in 15(1)(a);**
- **be supplied by the third party in confidence; and**
- **meet one of the harms or other conditions set out in 15(1)(c).**

Type of Record (section 15(1)(a))

In interpreting **section 15(1)(a)** the following concepts apply.

Third party business information is *explicitly* revealed if the information disclosed is itself third party business information or if it makes direct reference to third party business information. Third party business information is *implicitly* revealed if the information disclosed allows a reader to draw an accurate inference about third party business information (see *IPC Order 96-013* and *IPC Order 98-013*).

Trade secret is defined in **section 1(1)(s)** of the *Act* as information, including a formula, pattern, compilation, program, device, product, method, technique or process:

- that is used, or may be used, in business or for any commercial purpose;
- that derives independent economic value, actual or potential, from not being generally known to anyone who can obtain economic value from its disclosure or use;
- that is the subject of reasonable efforts to prevent it from becoming generally known; and
- the disclosure of which would result in significant harm or undue financial loss or gain.

Information must meet all of these criteria to be considered a trade secret.

Information that is generally available through public sources (e.g., corporate annual reports) would not usually qualify as a trade secret under the *Act*. A third party must also own trade secrets or must be able to prove a claim of legal right in the information (e.g., a licence agreement) in order for that information to qualify for the exception.

A *third party* is defined in **section 1(1)(r)** of the *Act* as any person, group of persons or organization other than the applicant (i.e., the person making an access request) or a public body.

The other terms in this section have their normal dictionary meanings.

Commercial information covers information concerning the sale, purchase or exchange of goods or services, such as pricing structures, market research, business plans, and customer records.

Financial information relates to money and its use or distribution or to assets with monetary value such as securities or stock options. Common examples are financial forecasts, investment strategies, budgets, and profit and loss statements.

Labour relations information relates to the management of personnel by a person or organization other than the applicant, whether or not the personnel are organized into bargaining units. Common examples of labour relations information are hourly wage rates, personnel contracts and information on negotiations regarding collective agreements.

Scientific information relates to experiments, principles and procedures derived by scientific method, including information such as designs for a product and testing procedures for drugs.

Technical information relates to particular subjects, crafts or professions that are based on a specific technique or approach. Examples are system design specifications and the plans for an engineering project.

Supplied "In Confidence" (section 15(1)(b))

Section 15(1)(b) covers information provided voluntarily by a third party and information provided by a third party under law or some other form of compulsion.

The information would normally have to be supplied by the third party and not compiled by the public body or generated jointly through negotiation with the public body (see *IPC Order 96-013*). **However, there may be exceptions where the information supplied to the public body during negotiations remains relatively unchanged in an agreement or could be inferred from an agreement** (see *IPC Order 2000-005)*.

For example, a report created by an inspector visiting a plant would not qualify as being supplied by the third party. On the other hand, a letter created by a public body might contain information that would qualify for exception if it reproduces or analyzes information supplied by a third party in such a way as to reveal the information itself (see *IPC Order 99-007*). Commercial information in a partnership agreement might also qualify for the exception if the information was originally supplied by a party to the agreement and has remained relatively unchanged in the agreement (see *IPC Order 2000-005*).

Implicitly in this context means that both parties understand the confidentiality. There may be no actual statement of confidentiality, no written agreement or other physical evidence of the understanding that the information will be kept confidential. In such cases, all relevant facts and circumstances need to be examined to determine whether or not there is an understanding of confidentiality.

Explicitly in this context means that there is documentary evidence that indicates that information was supplied on the understanding that it would be kept confidential.

In confidence usually describes a situation of mutual trust in which private matters are related or reported.

Some factors that may be considered when determining whether information was supplied implicitly or explicitly in confidence are:

- whether or not an explicit indication of confidentiality exists;
- the representations of the third party in reply to a third party notice as to their understanding of confidentiality;
- past practice of the public body, particularly whether similar information has normally been kept confidential in the past;
- the type of information, including the confidentiality with which it is maintained by the third party;
- whether the information was supplied voluntarily by the third party, at the request of the public body, or as required by law, and the consequences for the third party if it does not supply the information; and
- actions taken by, or conduct of, the public body and third party, which may indicate an understanding of confidentiality.

(See *IPC Order 97-013.*)

This guidance is provided to help a public body determine whether information is supplied in confidence. Where this is normal practice, persons and organizations submitting such information should be asked to mark records or parts of records as being submitted "in confidence."

It is the public body's responsibility to prove that information was submitted in confidence. It is not sufficient simply to accept a third party's stamp that documents are confidential or the assertion in representations that information was supplied in confidence. There must be evidence, such as that referenced above, to support the assertion or marking and to prove that the information has been treated consistently in a confidential manner.

Public bodies should review their understandings with third parties concerning the provision of information in confidence.

Effect on Business Interests (section 15(1)(c))

In applying **section 15(1)(c)**, there must be objective grounds for believing that one of the results listed below will occur as a consequence of disclosure. It must be shown that disclosure of the information would:

- significantly harm the third party's competitive position;
- interfere significantly with the third party's negotiating position;
- result in information no longer being supplied;
- result in undue financial loss or gain to any person or organization; or
- reveal information concerning the resolution of a labour relations dispute.

A refusal of access under this exception should be supported by detailed evidence showing that the expectation of harm is reasonable and the harm is probable. The evidence must show that:

- there is a clear cause and effect relationship between the disclosure and the alleged harm;
- the expected harm amounts to damage or detriment and not simply hindrance or minimal interference; and
- the likelihood of harm from disclosure of the specific information is genuine and conceivable, and not merely speculative; it is not sufficient to show that there is a potential for harm simply because the information is sensitive.

(See *IPC Order 96-003*.)

***Harm significantly the competitive position of a third party* (section 15(1)(c)(i)):** Harm *significantly* means that disclosure of the information will damage or cause detriment to the third party's competitive position and that the damage or detriment will have considerable impact on the third party involved.

In order to assess the significance of the harm, a public body should review, among other things:

- the nature of the information itself;
- the third party's representations regarding the harm involved;
- an objective appraisal of that harm, including any monetary or other value placed on it, if this can be determined;
- the impact on the third party and its ability to withstand this; and
- any public interest, as set out in **section 31**, which may affect the decision concerning disclosure.

***Interfere significantly with the negotiating position of a third party* (section 15(1)(c)(i)):** This provision allows for situations where disclosure of third party information would have a major impact on ongoing or future negotiations. Completed negotiations are not normally subject to the exception unless there is a good probability that the particular strategies will be used in the future and the disclosure of information relating to completed negotiations would reveal such strategies.

The intent of the provision is to protect a third party's ability to negotiate effectively with either the public body or other parties.

Examples would include negotiating positions, options, instructions and pricing criteria, and points used in negotiations.

***Result in similar information no longer being supplied to the public body when there is a continuing public interest that similar information continued to be supplied* (section 15(1)(c)(ii)):** This provision allows for situations where a third party may be so concerned by the possibility that information may be released that it refuses to supply similar information in the future. There must be a continuing public interest in the particular information being supplied. If this is the case, a public body can consider whether disclosure would discourage either the particular third party or another third party from voluntarily supplying information to it or other public bodies.

A third party may assert that it will no longer provide information if it may be released under the *FOIP Act*. However, the public body is required to come to a reasonable decision as to whether or not this will be the case. It is unlikely that similar information will no longer be supplied where the third party has a financial or other incentive to continue supplying the information or where it is legally required. (See *IPC Order 96-018*.)

Examples include voluntary supply of pricing information by a group of third parties which serves to effectively regulate pricing of products, and provision of information on leases and rental values of commercial property in order to apply market-value assessment across a city.

***Undue financial loss or gain to any person or organization* (section 15(1)(c)(iii)):** For this provision to apply, there must be objective grounds for believing that releasing the information would result in an undue loss or gain measured in monetary or monetary-equivalent terms (i.e., loss of revenue, loss of corporate reputation or loss of good will.

The undue financial loss or gain may apply to the public body that has custody or control of the information in question, the third party that supplied the information or any other person or organization.

There must be objective grounds for believing that the harm contemplated by this exception would actually result from disclosure. In refusing access under this provision, a public body should be prepared to present detailed and convincing evidence of the facts that led to the expectation that harm would occur if the information were disclosed. A link is required between the disclosure of specific information and the harm that is expected from the release.

***Reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute* (section 15(1)(c)(iv)):** This provision protects information which itself explicitly reveals a report of an arbitrator or other such person or directly makes reference to such a report, or which implicitly reveals information about such a report, by allowing a reader to draw an accurate inference about it. The report would have to deal with a labour relations dispute of a third party, not a public body.

A *report* may include a broad range of records providing information or opinions, or consisting of a formal statement or account of the results of an analysis of information. The recording of mere observation or a simple statement of fact would not generally be covered by this provision.

The provision requires that an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute create the report.

An *arbitrator* is generally considered to be a neutral person chosen by the parties to a dispute to hear their arguments and give judgment between them. The parties may submit themselves voluntarily or under a compulsory agreement to the decision of this person.

A *mediator* is a person who facilitates discussion between parties who disagree with the aim of reconciling them.

A *labour relations officer* is any person appointed to inquire into or resolve any form of labour relations dispute or issue.

Other persons or bodies appointed to resolve or inquire into a labour relations dispute includes any person or body appointed by any level of government or any public body; for example, Cabinet appointments, ministerial appointments, appointments by the council, board or the chief executive officer of a public body.

One example would be the ministerial appointment of a disputes inquiry board to attempt to resolve a dispute involving a school board. Another example would be the designation by the Director of the Labour Relations Board of a person requested by parties to a dispute as an officer of the Board.

Tax Information

Section 15(2) provides that a public body must refuse to disclose information about a third party that was collected on a tax return or collected for the purpose of determining tax liability or collecting a tax.

This is a mandatory exception and the public body has no discretion to release the information unless required to do so by law or by the provision in **section 31** for disclosure in the public interest.

Examples of such disclosure would be assessment or tax arrears information disclosed under the authority of the *Municipal Government Act*.

Information collected on a tax return is information on a form used to determine taxes to be paid for municipal, education, provincial or federal purposes, and includes corporate, business and personal tax information of a third party (see also section 4.4 of this chapter).

Collected for the purpose of determining tax liability means collected for the purpose of determining whether a person or organization owes past, present or future taxes to a school board, or a municipal, provincial or federal government.

Collected for the purpose of collecting a tax means collected by authorities for the purpose of collecting due or overdue taxes for a school jurisdiction, municipality or the provincial or federal government.

Section 15(2) may not be used to withhold an applicant's own tax information, since this is information about the company, organization or individual (e.g., sole proprietor) and not information about a third party.

This type of information commonly includes tax data derived from tax forms, audits of a business intended to determine whether or not taxes are owed, and information about directors of a bankrupt corporation gathered to determine who should be liable for taxes that are in arrears.

The exception may be used in relation to information concerning royalties or obtained in the process of collecting royalties. However, such royalties must have a statutory basis as a tax. Where there is doubt about the nature of a royalty, legal advice should be sought.

When the Exception Does Not Apply

Section 15(3) provides for situations where the exceptions set out in **section 15(1)** and **(2)** do not apply:

***If the third party consents to disclosure*:** A public body cannot withhold requested information under this exception when the third party concerned has consented to disclosure, although other exceptions may be applied to the information. Consent should be in writing. For details on consent see Chapter 5 of this publication dealing with third party notices.

If the third party neither consents nor objects to disclosure, the public body must assess the appropriate application of this exception. It always remains the responsibility of the public body to make the final decision, taking into consideration all relevant circumstances.

***If an enactment of Alberta or Canada authorizes or requires disclosure of the information*:** The information must be released where disclosure is provided for in other federal or provincial legislation.

***If the information relates to a non-arm's length transaction between the Government of Alberta and another party*:** This provision applies in circumstances where the Government of Alberta is a direct participant in a transaction and is working with the other party.

The definition of a non-arm's length transaction in **section 4(3)** of the *Act* is not applicable to this section. In this case, a *non-arm's length transaction* is a transaction between unrelated parties that has characteristics comparable to a transaction between related persons. The parties may be influenced in their bargaining by something other than individual self-interest, or one of the parties may have sufficient leverage or influence to exercise control or pressure on the free will of the other (see *IPC Order 98-013*).

An example would be an agreement between a corporation and the Government of Alberta to invest in and pursue a project together.

In this section, the *Government of Alberta* includes departments, branches and offices of the government and any agencies, boards, commissions, corporations, offices or other bodies listed in the FOIP Regulation.

***If the information is in a record that is in the custody or under the control of the Provincial Archives of Alberta or the archives of a public body and that has been in existence for 50 years or more*:** This provision recognizes that the sensitivity of business information decreases with time, and so does the injury that might occur to the business interests of a third party as a result of disclosure.

The fact that such information resides in the Provincial Archives or in the archives of a public body means that it is information important for research and historical purposes and that it should be available for those purposes after the passage of 50 years.

Disclosure of information can take place earlier if it would not be harmful to the business interests of a third party. See Chapter 7.11 of this publication for disclosure of information in archives.

Application of Exception

A number of steps are involved in considering whether or not information qualifies for an exception to disclosure under **section 15**. These are set out in ***Figure 1***.

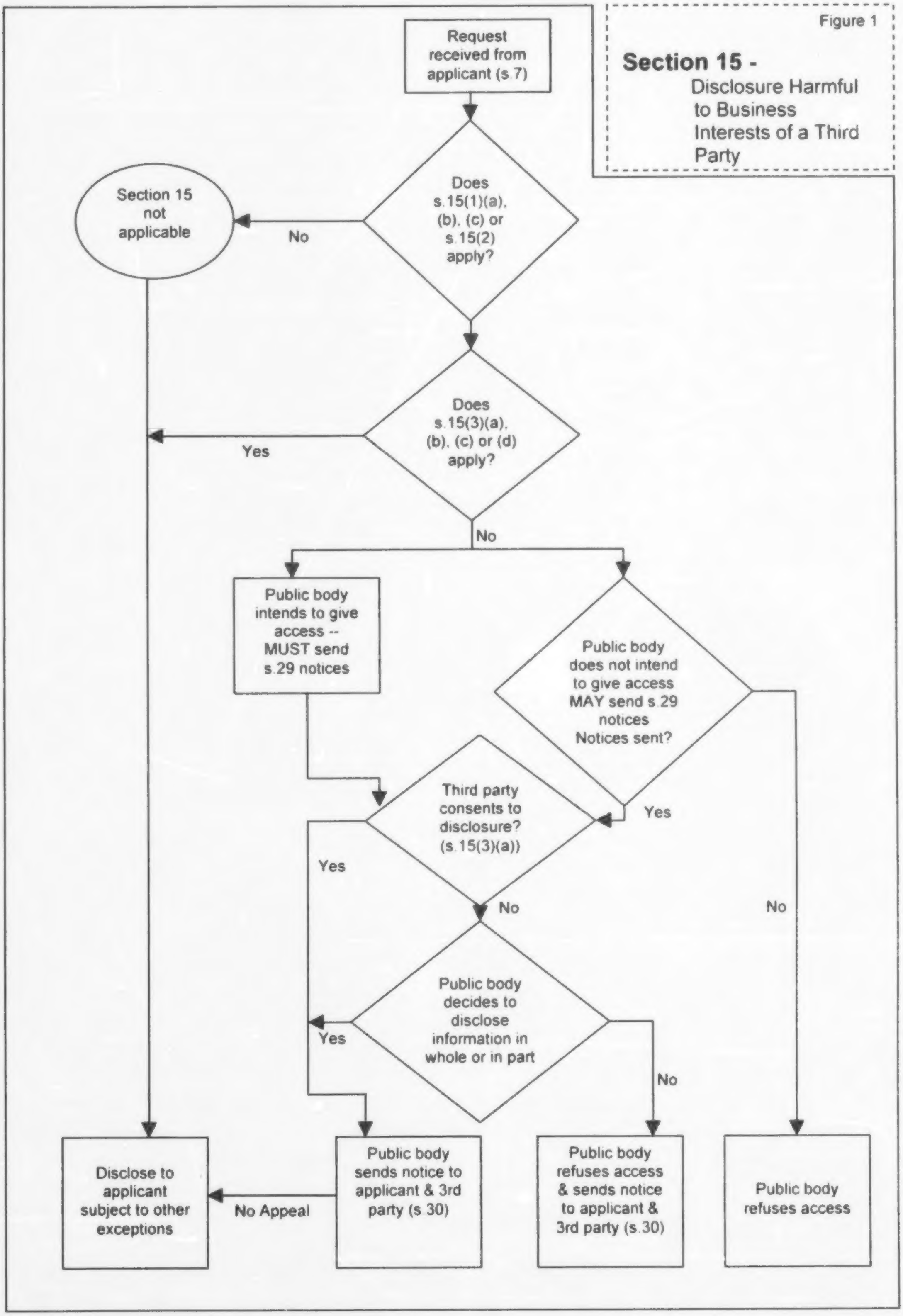


Figure 1

Section 15 - Disclosure Harmful to Business Interests of a Third Party

Request received from applicant (s.7)
Does s.15(1)(a), (b), (c) or s.15(2) apply?
No
Section 15 not applicable
Does s.15(3)(a), (b), (c) or (d) apply?
Yes
No
Public body intends to give access -- MUST send s.29 notices
Public body does not intend to give access MAY send s.29 notices Notices sent?
Yes
No
Third party consents to disclosure? (s.15(3)(a))
Yes
No
Public body decides to disclose information in whole or in part
Yes
No
Disclose to applicant subject to other exceptions
No Appeal
Public body sends notice to applicant & 3rd party (s.30)
Public body refuses access & sends notice to applicant & 3rd party (s.30)
Public body refuses access

4.4 DISCLOSURE HARMFUL TO PERSONAL PRIVACY

Overview

Section 16 of the *Act* protects the privacy of individuals whose personal information may be the subject of a FOIP request by someone else. This protection is provided by a mandatory exception for personal information when its release would constitute an unreasonable invasion of an individual's privacy.

In the exception the individual whom the information is about is referred to as a *third party*. This protection applies only to individuals and not to groups, organizations or corporations. The exception must always be considered when an applicant makes a request for someone else's personal information.

Any time someone other than the individual whom the information is about, or his or her representative, requests personal information as defined in section 1(1)(n) of the *Act*, it must be subjected to a test to determine whether disclosure would be an unreasonable invasion of a third party's personal privacy.

Definition of Personal Information

Personal information is defined as recorded information about an identifiable individual. A detailed definition is provided in Chapter 1.5 of this publication.

It is important to remember that the definition is non-exhaustive. The examples given are purely illustrative and do not define personal information in its entirety.

To qualify as personal information under the *Act*, information must be written, photographed, recorded, or stored in some manner. Information conveyed in a conversation that is not recorded does not constitute personal information for the purposes of the *Act*.

The personal information must be about an *identifiable individual*. It must be about an individual and not about a group of individuals, an organization or a corporation. The individual may be named in the record or it may be possible to ascertain or deduce the identity of the individual from the contents of the record.

Exception for Personal Information

Section 16(1) establishes a mandatory exception for personal information if disclosure of it would be an unreasonable invasion of a third party's personal privacy. When this is the case, the public body has no discretion to release the information.

Disclosure Not an Unreasonable Invasion of a Third Party's Privacy

Section 16(2) sets out those circumstances when disclosure of personal information is considered not to be an unreasonable invasion of a third party's personal privacy. **In these circumstances, a public body may not rely on section 16 to refuse disclosure of personal information**. However, other sections of the *Act* should still be considered when making a decision about disclosure.

Section 16(2) states that disclosure of personal information is not an unreasonable invasion of an individual's personal privacy if:

- the third party has, in writing, consented to or requested the disclosure;
- there are compelling circumstances affecting anyone's health or safety, and notice of the disclosure is mailed to the last known address of the third party;
- an Act of Alberta or Canada authorizes or requires the disclosure;
- the disclosure is for research or statistical purposes and is in accordance with **section 40** (research is discussed in Chapter 7 of this publication);
- the information is about the third party's classification, salary range, discretionary benefits or employment responsibilities as an officer, employee or member of a public body;
- the disclosure reveals financial and other details of a contract to supply goods or services to a public body;
- the disclosure reveals details of a licence, permit or other similar discretionary benefit that has been granted to a third party by a public body and relates to either a commercial or professional activity or to real property;
- the disclosure reveals details of a discretionary benefit of a financial nature granted to the third party by a public body;
- the personal information is about an individual who has been dead for 25 years or more; or
- the disclosure is not contrary to the public interest and reveals only the following information about a third party:
  - enrolment in a school of an educational body or in a program offered by a post-secondary educational body,
  - admission to a facility or institution of a health care body as a current patient or resident, except where the disclosure would reveal the nature of the third party's treatment,
  - attendance at or participation in a public event or activity related to a public body, including a graduation ceremony, sporting event, cultural program or club, or field trip, or
  - receipt of an honour or award granted by or through a public body.

The provisions of **section 16(2)** are discussed in more detail below.

Consent **(section 16(2)(a)):** Personal information may be released where the individual either consents to or requests the disclosure. This consent or request must be in writing and must be specific. Consent in such circumstances normally comes after third party consultation. Implied consent is not sufficient to satisfy this condition.

Consent can be provided to the public body on behalf of the individual by certain persons and under certain conditions as set out in **section 79** of the *Act*. The exercise of rights by others is discussed in detail in Chapter 7 of this publication.

Health and safety **(section 16(2)(b)):** This provision applies only when there are compelling circumstances affecting the health or safety of someone other than the third party. A *compelling circumstance* is one where there is no other way to protect someone else's health and safety, or where there is an emergency and disclosure is the fastest, most direct way to protect someone else's health or safety. The release of the information requested must also be likely to have a direct bearing on a compelling health or safety matter and it will be necessary to show this (see *IPC Order 98-007*).

In applying this provision, the public body is required to mail a notice of disclosure to the last known address of the third party whose personal information the public body is disclosing. This is the last address on file with the public body, unless circumstances are such that another public body or level of government may have a more recent address. The public body is required to make reasonable attempts to determine the address of the third party. **Model Letter Q** in Appendix 3 of this publication may be used in these situations.

***Act of Alberta or Canada* (section 16(2)(c)):** This provision states that personal information may be disclosed if disclosure is authorized or required by provincial or federal statute.

***Research purposes* (section 16(2)(d)):** This provision permits the disclosure of personal information for research or statistical purposes in accordance with provisions set out in **sections 40 or 41** of the *Act*. This recognizes that research may legitimately require the use of identifiable personal information, but ensures that the privacy rights of research subjects are protected.

Researchers have to comply with a stringent set of conditions. A full discussion of research agreements appears in Chapter 7.10 of this publication.

***Employment information about public officials* (section 16(2)(e)):** This provision sets special conditions for the release of particular employment information about officers, employees or members of public bodies. The rationale is that more information should be available about individuals who are paid out of public funds.

Section 1(1)(e) defines employee as including a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with a public body.

This includes all individuals appointed to boards or committees, those providing voluntary services on behalf of a public body, students who volunteer or are participating in a work-experience program and those employed under a personal services contract.

The provision establishes that the disclosure of information about the actual job classification and responsibilities of an employee, and information about the duties or job description for the position occupied is not an unreasonable invasion of an individual's personal privacy. This also applies to the release of the salary range for the position.

Where no salary range exists, public bodies should consider creating one in order to support release of information that promotes more accountability for the expenditure of public funds.

The provision also establishes that the disclosure of a discretionary benefit provided on an individual basis, rather than in accordance with a plan, scale or formula, including any allowance with monetary value that the public body chooses to provide, is not an unreasonable invasion of an individual's privacy.

An example might be a leave of absence granted to an employee who has been invited to serve as an officer of a professional association, if there is no provision for this in an applicable collective agreement or schedule of benefits for the employee's position.

***Contracts for goods and services* (section 16(2)(f)):** This provision establishes that the release of financial and other details about the supply of goods and services to a public body is not an unreasonable invasion of privacy, even when such details may be personal information.

The rationale is that the public is entitled to know from whom and for what amount such services were purchased. This is an important part of public accountability.

Financial details relates to the amounts paid under the contract. *Other details* includes the names of the parties, the subject of the contract and its terms and conditions.

Contract to supply goods and services refers to an agreement concluded by a public body with a third party to buy or sell products, merchandise, or services, as well as to an agreement entered into by a public body in relation to employment or performance of work-related duties. It does not apply where a public body provides money to a third party to provide contracted services to a party other than a public body (see *IPC Order 98-004*).

In releasing this type of information, public bodies should ensure that they are not disclosing information that may qualify for protection under **section 15**, information the disclosure of which would be harmful to third party business interests.

***Licence, permit or similar discretionary benefits* (section 16(2)(g)):** This provision establishes a mechanism for releasing information about discretionary benefits granted by a public body to a third party. Again the rationale is to ensure accountability on the part of public bodies with respect to monetary and other benefits that fall within its discretion.

Disclosure is limited to licences, permits or discretionary benefits relating to a commercial or professional activity, or to real property.

Licence or *permit* means authorization to carry out an activity, such as operating a particular establishment, or carrying on a professional or commercial activity. Examples would include business licences, teaching permits, taxi licences, and building and development permits.

Other similar discretionary benefit refers to both monetary and non-monetary benefits or allowances given by a public body. An example of this type of benefit would be the granting of a grazing lease for Crown land.

This provision does not allow disclosure of a licence or permit of a personal nature, such as a recreational fishing or hunting licence, a dog licence or a camping permit.

The benefit must be discretionary, that is, the public body must have a choice as to whether or not to provide the benefit or allowance.

The power to suspend, cancel or reinstate a licence or permit is an indication that the licence or permit is a discretionary benefit. So too is the power to limit or allocate permits by setting formulae or limiting numbers (see *IPC Order 98-014* and *IPC Order 98-018*).

Disclosure under this provision must reveal only the name of the person to whom the licence, permit or discretionary benefit is provided, and the nature of the benefit. It must not include personal information supplied in support of the application for the benefit.

***Discretionary benefit of a financial nature* (section 16(2)(h)):** This provision enables disclosure of information about a discretionary financial benefit provided to an individual by a public body.

A *discretionary benefit of a financial nature* is any monetary allowance that the public body chooses to provide (e.g., a scholarship or a grant). Information regarding eligibility for income assistance or social benefits, or regarding the determination of individual benefit levels, is not covered by this provision since these benefits are calculated according to entitlement formulae.

Background personal information required by the public body or provided voluntarily by the applicant must not be released under this provision.

An example of this type of disclosure would be the disclosure of records that show that an individual has received a grant from a public body, the amount of the grant and the purpose for which the grant will be used. Personal information supporting the application for the grant itself would not be disclosed.

***Individual dead for 25 years or more* (section 16(2)(i)):** This provision puts a time limit on the protection of privacy after death. Once an individual has been dead 25 years or more, release of his or her personal information is deemed not to be an unreasonable invasion of the individual's privacy. The provision is particularly important for permitting historical and genealogical research.

The onus is on the applicant to produce evidence that an individual has been dead for 25 years or more.

***Disclosure not contrary to the public interest* (section 16(2)(j)):** This provision allows for disclosure of limited personal information that has historically been available to the public.

"Public interest" in **section 16(2)(j)** is not intended to be subject to the same test as is applied in relation to **section 31(1)(b)** or **section 87(4)(b)**. Public bodies must take into account the circumstances surrounding the request.

If the information could be used to commit a criminal act or harm an individual or property, then it is likely to be contrary to the public interest to disclose the information. If a disclosure would reveal information about the mental or physical health of individuals, or affect their mental or physical health, the disclosure may be contrary to the public interest.

When determining whether information should be disclosed, public bodies should review the other exceptions in the *Act* to determine whether any of them also apply to the information.

***Enrolment in school, or in a program of post-secondary body* (section 16(2)(j)(i)):** This provision allows a school board, charter school or regional school authority to confirm that an individual is or was enrolled in a school under its jurisdiction. A post-secondary educational body can confirm that an individual is or was enrolled in a specific program at that institution. Educational bodies may also provide lists or class photographs of the individuals enrolled in a particular school or post-secondary program whether currently or in the past (e.g., the students in a particular high school or the students in a particular apprenticeship program). This facilitates school or program reunions.

This provision does not allow disclosure of whether or not an individual is actually in attendance at a school or post-secondary institution at a particular time. Nor does it allow disclosure of an individual's timetable of studies or other personal information related to his or her educational program.

***Admission to a health care facility* (section 16(2)(j)(ii)):** This provision allows a public body to confirm that an individual has been admitted to a hospital or is living in a long-term care facility. A nursing home may also provide a list of residents of the facility. Other public bodies may provide information on the admission of a person to a hospital following an accident or after ambulance transportation.

Section 16(2)(j)(ii) does not authorize health care bodies to provide information about an individual who is no longer resident in a long-term care facility or no longer receiving treatment in a hospital. The patient or resident would have to be in the treatment facility or nursing home on the date of the FOIP request.

This provision also does not allow health care bodies to disclose the nature of an individual's treatment. Information that would reveal the specific details of particular wards, courses of treatment or special units cannot be released under this provision.

It should be noted that health legislation that is paramount over the *FOIP Act* (see the FOIP Regulation, **section 15(2)**) may further restrict or prohibit disclosure of information relating to persons admitted to a health care facility.

***Attendance or participation at a public event or public activity* (section 16(2)(j)(iii)):** This provision allows disclosure of the names of individuals who are recorded as having attended or participated in a public event or activity.

A *public event or activity* is something that is noteworthy, supervised or organized in some way. It would be open, or accessible, to the public:

- without restriction, or
- with limited attendance due to space or safety concerns, or
- through ticket sales.

The fact that someone was simply observed or something was seen happening does not make an occasion a public event or activity. The *Act* is based on recorded information, so a record of the attendance or participation is needed for disclosure under this provision.

This provision does not relate to:

- events or activities that are organized or sponsored by a third party that may be renting a facility owned by a public body;
- events that are not authorized or sponsored by a public body; or
- activities of arm's-length bodies such as "Foundations" or "Friends," unless the record is in the custody of the public body.

Disclosure is not limited to current events, but also includes past events if records exist. Photographs taken at the event may be disclosed. It is important that reasonable steps are taken to ensure that records of such activities which are maintained by public bodies are accurate.

***Receipt of an honour or award granted by or through a public body* (section 16(2)(j)(iv)):** This provision allows the disclosure only of the receipt of an honour or award. This means that the individual must have actually received the honour or award. This provision does not allow disclosure of offers or qualification for an honour or award if it was not presented, or an award that an individual has declined.

A public body can confirm that a particular honour or award has been given to an individual and can disclose a list of names of individuals who have received a particular honour or award. Disclosure of a photograph of an individual named as a recipient of a current or past award would also be allowed under this provision.

Request for Non-Disclosure of Personal Information

Section 16(3) allows an individual to request that information described in **section 16(2)(j)** not be disclosed.

If such a request is made, it is an unreasonable invasion of personal privacy to disclose any of the information that the individual has requested not be disclosed. This may include all the information contemplated under **section 16(2)(j)** or just parts of that information.

A public body cannot use this provision as a blanket provision to refuse disclosure. **Section 16(3)** must be applied on an individual basis to ensure that nothing is done that could detrimentally affect the confidence and respect that the public has in the ability of public bodies to protect personal information. At the same time, public bodies should avoid causing uncertainty or confusion in the public mind about whether disclosure will or will not take place.

For these reasons, it is advisable for public bodies to notify individuals that they have this right under the *Act* so that they can exercise the right if they wish.

Public bodies should also ensure that procedures are in place so that requests for non-disclosure can be honoured and that no inadvertent disclosure of personal information takes place.

Unreasonable Invasion of Privacy

Section 16(4) sets out particular types of personal information the disclosure of which is *presumed* to be an unreasonable invasion of a third party's personal privacy. That is to say, the legislation indicates that there is a likelihood that disclosure of such information might lead to an unreasonable invasion of privacy.

This provision creates a presumption that may be overridden by evidence to the contrary. In such instances, the burden of proof is on the applicant to provide evidence that could override the presumption.

Section 16(4) provides that disclosure of personal information is presumed to be an unreasonable invasion of a third party's privacy if the personal information:

- relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation;
- is an identifiable part of a law enforcement record, except to the extent that disclosure is necessary to dispose of the law enforcement matter or to continue an investigation;
- relates to eligibility for income assistance or social services benefits or to the determination of benefit levels;
- relates to an individual's employment or educational history;
- was collected on a tax return or gathered for the purpose of collecting a tax;
- consists of personal recommendations or evaluations, character references or personnel evaluations;
- consists of the third party's name when:
  - it appears with other personal information about the third party; or
  - the disclosure of the name itself would reveal personal information about the third party; or
- indicates the third party's racial or ethnic origin, or religious or political beliefs or associations.

Generally, these types of personal information tend to be of a particularly sensitive or delicate nature.

In interpreting this provision, the following explanations should be considered.

***Medical, psychiatric or psychological information* (section 16(4)(a))** covers records relating to an individual 's physical, mental or emotional health, including, for example, diagnostic, treatment and counselling information.

***Law enforcement* (section 16(4)(b))** covers investigations and proceedings relating to offences under the *Criminal Code* (Canada), breaches of other federal and provincial statutes and regulations, contravention of municipal by-laws, and formal security or administrative investigations carried out by a public body.

Disclosure of personal information in a law enforcement record is not presumed to be an unreasonable invasion of privacy if disclosure is necessary to dispose of the law enforcement matter or to continue the investigation.

This provision recognizes that a public body that is in possession of evidence relating to a law enforcement matter must have the power to disclose that evidence to the police, another law enforcement agency and to Crown counsel or other persons responsible for prosecuting the offence or imposing a penalty or sanction.

***Income assistance and social benefits* (section 16(4)(c))** relates to monetary benefits provided by municipal, federal or provincial governments to augment an individual's earnings, as well as non-monetary contributions that help supplement earnings from another source. Disclosure of such information is presumed to be an unreasonable invasion of personal privacy.

Relate here means that a connection or association must be established between the personal information and the eligibility or determination.

Eligibility means that the personal information must relate to whether a person qualifies to receive income assistance or social service benefits.

Determination of benefit levels means that the personal information must relate to a determination of how much benefit a person receives (see *IPC Order 98-004*).

***Employment history* (section 16(4)(d))** refers to any information regarding an individual's work record, including the name of an employer, past and present, the term of employment, the duties associated with a position, the salary and reasons for leaving, and any evaluation of job performance.

This presumption of unreasonable invasion of privacy does not apply to some employment information about officers, employees and members of public bodies (see above, Employment information about public officials (**section 16(2)(e)**).

***Educational history* (section 16(4)(d))** refers to any information regarding an individual's schooling and formal training, including names of schools, colleges or universities attended, courses taken, and results achieved. **The presumption of unreasonable invasion of privacy does not apply to certain information about enrolment in a school or program or the receipt of honours or awards** (see above, Disclosure not contrary to the public interest (**section 16(2)(j)**).

***Personal information collected on a tax return or gathered for the purpose of collecting a tax* (section 16(4)(e))** means personal information on a form used to calculate or report tax to be paid. It applies whether the tax return form was used to collect municipal, education, federal, or provincial taxes.

Gathered for the purpose of collecting a tax means collected by authorities for the purpose of collecting due or overdue municipal, education, federal, or provincial taxes.

***Personal recommendations, evaluations, and character references* (section 16(4)(f))** refers to both the assessment of employment potential and vouching for an individual's good character within the employment context. It also extends to recommendations or character references required by landlords and assessments of character for positions of trust. A formal process of conducting the assessment or evaluation is implied.

Personnel evaluations arise most often in the employment context and include job performance appraisals and absenteeism reports.

***Name of individual* (section 16(4)(g))** refers to situations where disclosure of an individual's name can be an unreasonable invasion of personal privacy if it is connected to other information about the individual. The name by itself may have attributes that reveal information about the individual (e.g., gender, race or ethnic origin).

***Racial or ethnic origin or religious or political beliefs or associations* (section 16(4)(h)):** *Racial origin* means information identifying common descent that connects a group of persons (e.g., Mongolian race or Caucasian descent).

Ethnic origin is similar to racial origin in that it identifies a common descent that connects a group of persons but extends to other common attributes such as language, culture or country of origin.

Religious or political beliefs refers to an individual's opinions about religion or a political party, an individual's membership or participation in a church, a religious organization or political party or an individual's association or relationship with a church, a religious organization (including native spirituality), or a political party.

Associations refers broadly to relationships with organizations such as labour unions.

Determination of Unreasonable Invasion of Privacy

Section 16(5) of the *Act* sets out criteria for determining whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy. It provides that, in determining whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy under **sections 16(1)** or **(4)**, a public body must consider all the relevant circumstances.

These include whether:

- the disclosure is desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny;
- the disclosure is likely to promote public health and safety or the protection of the environment;
- the personal information is relevant to a fair determination of the applicant's rights;
- the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people;
- the third party will be exposed unfairly to financial or other harm;
- the personal information has been supplied in confidence;
- the personal information is likely to be inaccurate or unreliable;
- the disclosure may unfairly damage the reputation of any person referred to in the record requested by the applicant; and
- the personal information was originally provided by the applicant.

This list is not exhaustive.

In applying **section 16(5)** a public body is required to consider not only the specific criteria set out in the provision but *all the relevant circumstances*. It must consider the sensitivity of the personal information in the context in which it was collected or compiled and the circumstances governing its continued protection or disclosure (see *IPC Order 96-021* and *IPC Order 98-004*).

For example, the sensitivity of a person's name and address in relation to a contagious disease would normally be protected for a very long period of time.

However, if disclosure is necessary to protect public health and safety, the personal information could be disclosed. Disclosure is permitted if consideration of all the relevant circumstances leads the public body to conclude that the disclosure is not unreasonable in the specific case. As the example demonstrates, the criteria set out in **section 16(5)** may, in exceptional circumstances, dictate the disclosure of the sensitive types of personal information described in **section 16(4)**, despite the fact that disclosure of such information is *normally* considered an unreasonable invasion of a third party's personal privacy.

The provisions of **section 16(5)** are discussed in more detail below.

***Public scrutiny* (section 16(5)(a)):** This provision recognizes that, in some cases, the desirability of public scrutiny of the internal workings of a public body will prevail over the protection of personal privacy (see *IPC Order 97-002*).

Public scrutiny is not necessarily limited to instances where wrongdoing is alleged or where it is alleged that the public body's normal practices and procedures are not being followed. It may be appropriate to disclose some personal information in order to demonstrate that the law is being properly enforced or public policy being carried out.

The public body should consider the broader interest of public accountability that may be advanced by disclosure of the requested information. For example, personal information about a successful job applicant may be disclosed to demonstrate that a qualified individual was appointed to a post and that the competitive process is working in a satisfactory manner.

***Public health, safety and protection of the environment* (section 16(5)(b)):** These public interests provide powerful override criteria for assuring protection of the general public interest.

Public health refers to the well being of the public at large. The test is whether the level of physical, mental or emotional health of all or a significant part of the public would be maintained or improved by the disclosure of particular personal information.

Public safety refers to the safety or well-being of all or a significant part of the public. This test centres on whether disclosure of personal information would reduce the community's exposure to a particular risk or danger.

Protection of the environment refers to guarding or defending all components of the earth – including air, land, and water; all layers of the atmosphere; all organic and inorganic matter and the interacting natural systems that include components of these things – from degradation through illegal or improper use.

***Determination of an applicant's rights* (section 16(5)(c)):** There may be occasions where the applicant requires access to personal information about someone else in order to assist in determining his or her own rights. Motives for requesting information are not normally relevant to the processing of a request. However, if it appears that the personal information is being requested for this purpose, it will be necessary for the applicant to confirm that this is the case. The interests of the applicant and the privacy interests of the third party will then have to be weighed to decide whether disclosure of personal information is essential to a fair determination of the applicant's rights.

The disclosure requires that the information be *relevant* to a *fair determination* of the applicant's rights. This means that the personal information requested must have a direct bearing on those rights and that, without the personal information, the applicant will probably not be able to resolve outstanding issues in a just and equitable manner. An important factor is whether there are other ways to obtain the required information.

Applicant's rights refers to any claim, entitlement, privilege or immunity of the applicant who is requesting someone else's information. For example, disclosure of third party personal information may be necessary so that an individual can prove his or her inheritance rights.

If an applicant has agreed to waive future claims on a matter, the applicant has no rights to be determined and cannot rely on this provision to pursue the matter (see *IPC Order 98-008*).

***Claims, disputes or grievances of aboriginal people* (section 16(5)(d)):** There may be a need to disclose personal information about individuals in order to research the background and expedite the settlement of wider rights for aboriginal people.

Validating means the confirming of rights that have been contended by the parties to a claim, dispute or grievance.

The phrase *claims, disputes and grievances* is interpreted broadly to include all manner of controversies, debates and differences of opinions regarding issues, and is not restricted to differences over land claims.

Aboriginal people means individuals whose racial origins are indigenous to Canada.

***Exposure to financial or other harm* (section 16(5)(e)):** There may, from time to time, be circumstances where disclosure of personal information may mean that the individual involved will be exposed unfairly to monetary loss or injury of a similar nature.

For example, release of partial or inconclusive test results about an individual may result in loss of his or her employment. In such circumstances, a public body should opt for protecting personal privacy.

Disruption of family relationships or damage to the reputation of deceased individuals may also constitute harm (see *IPC Order 98-007*).

***Personal information supplied in confidence* (section 16(5)(f)):** There are circumstances where personal information is supplied in a setting of trust and in the confidence that it will not be disclosed. Sometimes this understanding is more *implicit* than *explicit* and, in such circumstances, the public body should attempt to protect the personal privacy of the third party.

Some factors to consider when determining whether or not personal information was supplied in confidence are:

- the existence of a statement or agreement of confidentiality, or lacking this, evidence of an understanding of confidentiality;
- the understanding of a third party as set out in his or her representations as a result of third party notice;
- past practices in the public body, particularly in regard to keeping similar personal information confidential;
- the type of personal information, especially its sensitivity and whether it is normally kept confidential by the third party; and
- the conditions under which the information was supplied by the third party, voluntarily or through informal request by the public body or under compulsion of law or regulation, and the expectations created by the receipt or collection process.

The burden of determining whether or not information was supplied in confidence lies with the public body.

Public bodies should ask their clients and organizations with which they are

dealing to mark as confidential any records or parts of records containing personal information which are being supplied in confidence.

However, it is not sufficient for a public body to simply accept the stamp or assertion of a third party for confidentiality. **There must be evidence to support the assertion and to prove that the personal information has been treated consistently in a confidential manner.**

***Inaccurate or unreliable personal information* (section 16(5)(g)):** A public body may have inaccurate personal information in its custody or under its control for a variety of reasons. It may have been incorrectly recorded at the time of collection or compilation or it may have become inaccurate with the passage of time or as a result of a change in circumstances.

For these or other reasons, the public body may be unsure of the reliability of personal information. Such personal information should be disposed of under approved records disposition processes. Otherwise, no personal information should be disclosed from such records until the individual concerned has consented and verified that the information is correct.

***Unfairly damage reputation* (section 16(5)(h)):** If disclosure of personal information will unfairly damage the reputation of an individual, it should not be disclosed (see *IPC Order 97-002*).

Unfairly has the normal meaning of without justification, legitimacy or equity.

Damage the reputation of a person means to harm, injure or adversely affect what is said or believed about the individual's character. An example would be the disclosure of allegations of sexual harassment against an individual before an internal investigation is concluded.

***Personal information originally provided by the applicant* (section 16(5)(h)):** The applicant may have provided information about an individual because the individual was in the applicant's care or custody at the time. It is particularly relevant if the applicant and the other individual have no adverse interests at the time of the request.

Examples include personal information provided to a public body by an applicant who had guardianship or trusteeship of an individual and provided the information as a part of that responsibility (see *IPC Order 98-004*).

Existence of Record

In some instances, disclosure of the mere fact that a public body maintains a record on a third party may be an unreasonable invasion of a third party's privacy.

Section 11(2)(b) of the *Act* provides that a public body may, in response to an applicant, refuse to confirm or deny the existence of a record containing personal information about a third party, if disclosing the existence of the information would be an unreasonable invasion of the third party's personal privacy.

Most public bodies will use this provision in rare instances. However, public bodies that hold sensitive personal information, such as medical or financial information, may routinely refuse to confirm or deny the existence of records containing personal information about a third party.

When the existence of a record is neither confirmed nor denied, the response to the applicant required under section 11(1) must incorporate a statement as provided for in Model Letter I in Appendix 3 of this publication.

A refusal to confirm or deny the existence of a record is a significant limit to the right of access. If an applicant asks the Information and Privacy Commissioner to review a refusal to confirm or deny the existence of a record, the public body will be required to provide detailed and convincing reasons why **section 11(2)** was applied.

Before refusing to confirm or deny the existence of a record, a public body is expected to determine whether or not any record exists in order to properly fulfil its duty to assist the applicant (see *IPC Order 98-009*).

Application of Exception

The application of **section 16** is set out in ***Figure 2***.

A detailed explanation of the procedures relating to third party notice which apply to this exception is provided in Chapter 5 of this publication.

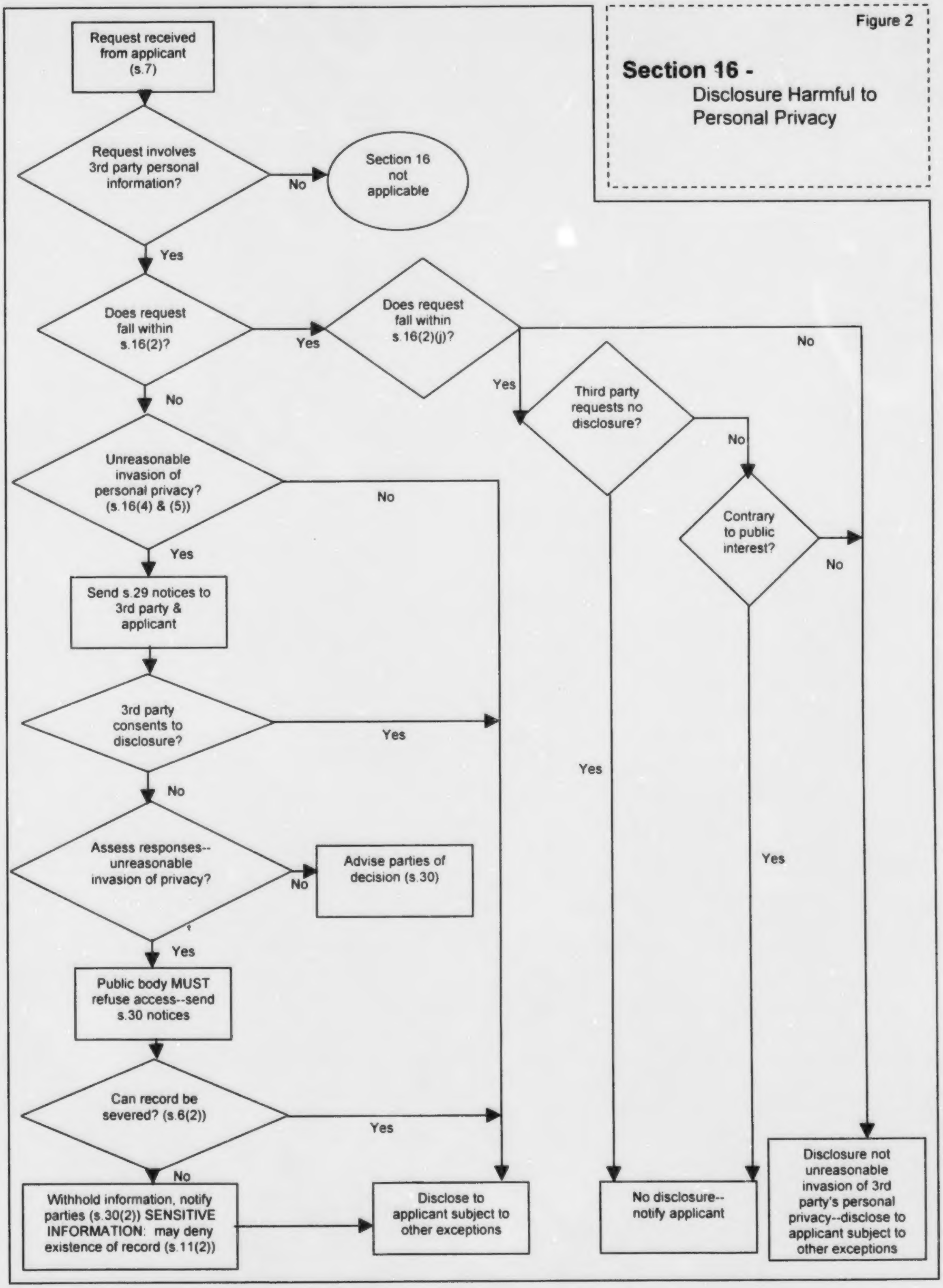


Figure 2

Section 16 -
Disclosure Harmful to Personal Privacy

Request received from applicant (s.7)
Request involves 3rd party personal information?
No
Section 16 not applicable
Yes
Does request fall within s.16(2)?
Yes
Does request fall within s.16(2)(j)?
No
Yes
Third party requests no disclosure?
No
Contrary to public interest?
No
No
Unreasonable invasion of personal privacy? (s.16(4) & (5))
No
Yes
Send s.29 notices to 3rd party & applicant
3rd party consents to disclosure?
Yes
Yes
No
Assess responses--unreasonable invasion of privacy?
No
Advise parties of decision (s.30)
Yes
Yes
Public body MUST refuse access--send s.30 notices
Can record be severed? (s.6(2))
Yes
No
Withhold information, notify parties (s.30(2)) SENSITIVE INFORMATION: may deny existence of record (s.11(2))
Disclose to applicant subject to other exceptions
No disclosure--notify applicant
Disclosure not unreasonable invasion of 3rd party's personal privacy--disclose to applicant subject to other exceptions

4.5 DISCLOSURE HARMFUL TO PUBLIC OR INDIVIDUAL SAFETY

Section 17 of the *Act* allows a public body discretion to refuse to disclose information when the disclosure is likely to threaten individual or public health or safety.

Section 17 is a discretionary exception.

Section 17(1) allows discretion to refuse to disclose information to an applicant if that disclosure could reasonably be expected to:

- threaten anyone else's safety or physical or mental health, or
- interfere with public safety.

The exception may extend to an applicant's own personal information as well as to information about third parties.

Threaten means to expose to risk or harm, and *safety* implies relative freedom from danger or risks.

Mental health refers to the functioning of a person's mind in a normal state.

Physical health refers to the well-being of an individual's physical body.

The mental or physical health of a person would be threatened if information were disclosed to an applicant that would cause severe stress to the person's mind or body.

In making determinations about mental or physical health, a public body may consult with its own health or other qualified professional staff, or consult a duly qualified health professional outside the public body to help arrive at a decision.

Individual safety could be threatened if information were released that allowed someone who had threatened to kill or injure the individual to locate him or her. Examples of individuals whose safety might be threatened would include an individual fleeing from a violent spouse, a victim of harassment or a witness to harassment, an employee who has been threatened during a work dispute or harassment case, and an individual in a witness protection program.

Mental or physical health might be threatened if information were disclosed to the applicant that could cause an individual to become suicidal or that could result in verbal or physical harassment or stalking.

Interference with public safety would occur where the disclosure of information could reasonably be expected to hamper or block the functioning of organizations and structures that ensure the safety and well-being of the public at large.

Section 17(2) specifically allows discretion to refuse to disclose to an applicant his or her own personal information if the disclosure could reasonably be expected to result in immediate and grave harm to the applicant's health or safety. The decision must be supported by the opinion of a physician, chartered psychologist, psychiatrist or other appropriate expert, depending on the circumstances of the case.

Immediate and grave harm to an applicant's health or safety means serious physical injury or mental trauma or danger to the applicant that could reasonably be expected to ensue directly from disclosure of the personal information.

This is an exception that is rarely used. It is important that the exception is based on the immediate and substantial harm that would result from the disclosure of information to the individual.

Section 5 of the FOIP Regulation governs the use of experts in providing individuals with very sensitive information about themselves. When using this section, the public body must have an agreement in place to ensure that the expert maintains the confidentiality of the information. If a copy of any record is provided to the expert, it must be returned to the public body or disposed of in accordance with the agreement.

An example where this exception may be relevant is where an individual with a long and difficult history of mental instability might suffer grave mental or physical trauma if certain diagnoses were made available to him or her without the benefit of medical or mental health intervention.

Though the intent of **section 17(2)** is to ensure that the applicant does not receive personal information that might cause immediate and grave trauma, efforts should be made to provide to the applicant as much of his or her own personal information as possible.

After obtaining the expert opinion, the public body may require that the applicant who has requested access to a record examine that record in person, and in the presence of someone who can clarify the information and assist the applicant in understanding it. That person may be a medical or other expert, a member of the applicant's family, or some other person approved by the public body (**section 5(5)** of the FOIP Regulation).

Section 17(3) allows discretion to refuse to disclose information that reveals the identity of an individual who has provided confidential information about a threat to someone's safety or mental or physical health.

This provision allows a public body to protect the identity of experts and of informants who provide such information. Examples of individuals whose identity might have to be protected include a person reporting abuse under the *Protection for Persons in Care Act*, a person reporting suicidal tendencies of a student, or an individual reporting that someone with AIDS is having unprotected sexual relations.

Existence of Record

In some instances, disclosure of the mere fact that a public body maintains a record may reasonably be expected to threaten someone else's safety, interfere with public safety, or even cause harm to the applicant.

Section 11(2)(a) of the *Act* provides that a public body can refuse to confirm or deny the existence of a record containing information described in **section 17**.

When the existence of a record is neither confirmed nor denied, the response to the applicant, as required under section 11(1), must incorporate a statement as provided for in Model Letter I in Appendix 3 of this publication.

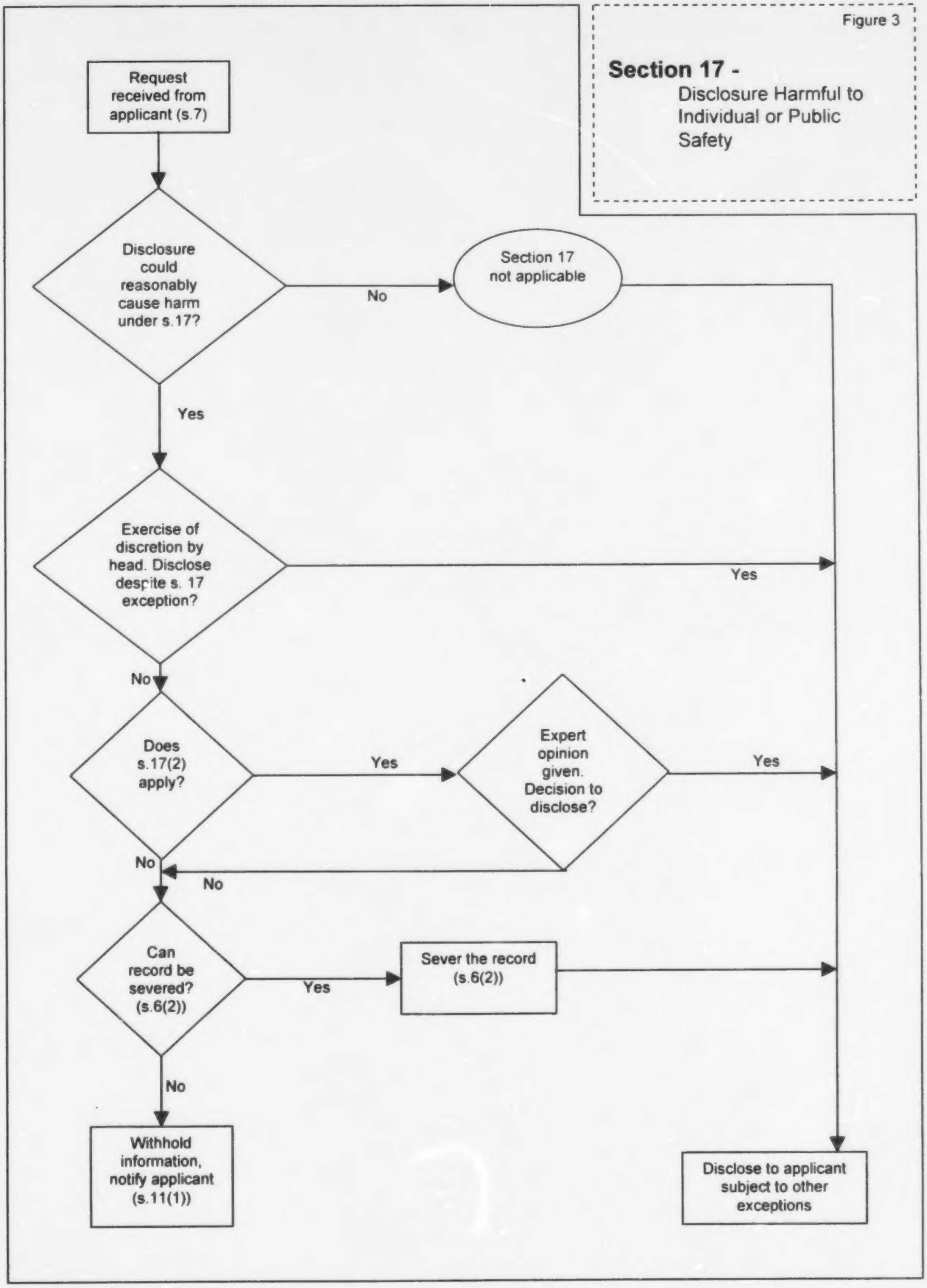
See section 4.4 of this chapter, Existence of a Record, for further information on the use of **section 11(1).**

Application of Exception

Figure 3 contains a flowchart setting out the application of **section 17**.

Figure 3

Section 17 -
Disclosure Harmful to Individual or Public Safety


Request received from applicant (s.7)
Disclosure could reasonably cause harm under s.17?
No
Section 17 not applicable
Yes
Exercise of discretion by head. Disclose despite s. 17 exception?
Yes
No
Does s.17(2) apply?
Yes
Expert opinion given. Decision to disclose?
Yes
No
No
Can record be severed? (s.6(2))
Yes
Sever the record (s.6(2))
No
Withhold information, notify applicant (s.11(1))
Disclose to applicant subject to other exceptions

4.6 CONFIDENTIAL EVALUATIONS

Section 18 of the *Act* provides that a public body may refuse to disclose confidential evaluative information or opinions to an applicant in certain circumstances.

Section 18 is a discretionary exception and **applies only when an individual, or a representative acting on his or her behalf, is requesting his or her own personal information.** The exception applies to both the applicant's own personal information and the personal information of the individual supplying the evaluation or opinion.

The application of **section 18(1)** is subject to a three-part test:

- the information must be evaluative or opinion material;
- it must be compiled for the purpose of determining the applicant's suitability, eligibility or qualifications for employment or for the awarding of contracts or other benefits; and
- the information must be provided, explicitly or implicitly, in confidence.

This provision protects the process where information is compiled about an individual in order to assess his or her suitability for either employment or the awarding of contracts or other benefits. This may involve information on his or her personal strengths or weaknesses, or eligibility (fitness or entitlement), or qualifications (attainments and accomplishments).

The exception applies only to the selection process and not to evaluative processes relating to other aspects of employment or the awarding of contracts or benefits.

Employment refers to selection for a position as an *employee* of a public body, as defined in the *Act* (**section 1(1)(e)**).

Contracts refers to agreements relating to both personal services and the supply of goods and services.

Other benefits refers to benefits conferred by a public body through an evaluative process. The term includes research grants, scholarships and prizes. It also includes appointments required for employment in a particular job or profession such as a bailiff or special constable (see *IPC Order 98-021*).

The term is not intended to refer to admission to programs of study, student or low-income housing, or benefits based solely on objective criteria.

For this exception to apply, the personal information must be contained in a confidential evaluation or opinion provided to the public body, but a summary of an evaluation that is compiled by the public body would also qualify (see *IPC Order 98-021*).

Examples of such evaluations include:

- a verbatim transcription of a reference check of an employment candidate, supplied in confidence; and
- a summary of a mix of telephone and written reference checks compiled by an official.

An analysis of the interview or of all reference checks prepared by the public body would not be excepted under this provision. Factual information such as statistics on absenteeism would also not be excepted.

Section 18(2) deals with the personal information of participants in a formal employee evaluation process concerning the applicant.

Participant is defined in **section 18(3)** as including a peer, subordinate or client of the applicant. **It does not include the applicant's supervisor or superior.**

Public bodies that incorporate "360 degree" evaluations into performance appraisals may withhold the names and positions of subordinates or colleagues, or the identity of students or clients of the applicant. In certain situations, such as those involving a very small review group, some or all of the evaluative comments may reasonably be expected to reveal the identity of the reviewer and may be excepted.

Section 18(2) is not intended to allow the withholding of the evaluative or appraisal information itself.

For either **section 18(1)** or **section 18(2)** to apply, the information must be provided with either an explicit or implicit understanding that it will be held in confidence. This intention that confidentiality will be maintained may be explicitly stated in the record itself or in an agreement governing the process, or implied by the circumstances under which the information is submitted and received.

Where confidentiality is implied, there must be objective grounds to support the assumption of confidentiality. It is not sufficient for the submitting party simply to stamp documents "Confidential." Public bodies are encouraged to have written policies dealing with the anonymity or absence thereof in such processes, and procedures in place to protect such anonymity.

Some factors that may be considered when determining whether information was received in confidence are set out in section 4.2 of this chapter.

Figure 4 contains a flowchart setting out the application of **section 18**.

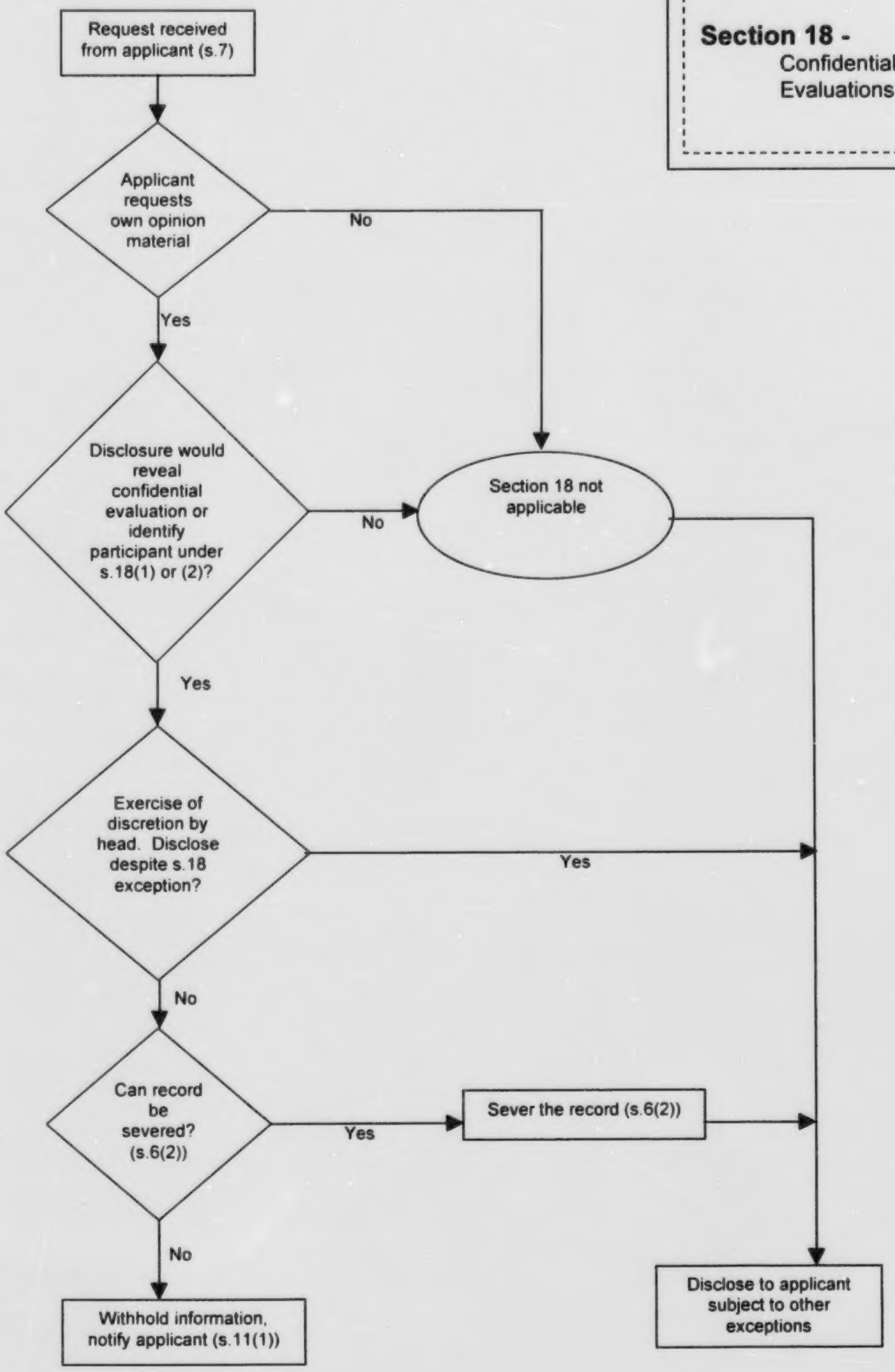


Figure 4

Section 18 - Confidential Evaluations

Request received from applicant (s.7)
Applicant requests own opinion material
No
Yes
Disclosure would reveal confidential evaluation or identify participant under s.18(1) or (2)?
No
Section 18 not applicable
Yes
Exercise of discretion by head. Disclose despite s.18 exception?
Yes
No
Can record be severed? (s.6(2))
Yes
Sever the record (s.6(2))
No
Withhold information, notify applicant (s.11(1))
Disclose to applicant subject to other exceptions

4.7 DISCLOSURE HARMFUL TO LAW ENFORCEMENT

Overview

Section 19 of the *Act* deals with the application of exceptions to protect both law enforcement activities and information in certain law enforcement records. It contains a number of discretionary exceptions, and a mandatory exception requiring public bodies to refuse to disclose information if this would be an offence under an Act of Canada.

Several provisions of the *Act* that relate to law enforcement were affected by amendments that came into force in May 1999. For separate treatment of the effect of these amendments, see *FOIP Bulletin No. 7, Law Enforcement*.

Law enforcement is defined in **section 1(1)(h)** of the *Act* as:

- policing, including criminal intelligence operations,
- a police, security or administrative investigation, including the complaint that gives rise to the investigation, that leads or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred, or
- proceedings that lead or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred.

Policing refers to the activities of police services. It includes investigations of offences, prevention of crime, maintenance of law and order, security and protective services, and law enforcement research and analysis.

Criminal intelligence is information relating to a person or group of persons. It is compiled by police services to anticipate, prevent or monitor possible criminal activity.

Intelligence-gathering is sometimes a separate activity from the conduct of investigations. Intelligence may be used for future investigations, for activities aimed at preventing the commission of an offence, or to ensure the security of individuals or organizations.

Investigation refers to a systematic process of examination, inquiry and observation. It includes the complaint that leads to the investigation. The phrase *lead or could lead* indicates that investigations are part of law enforcement even if they do not actually result in proceedings in a court or tribunal.

A public body need not carry out the investigation for that investigation to meet the definition. The records must, however, be in the custody or control of a public body.

The definition includes the complaint that gives rise to an investigation. This means that the initial complaint receives the same consideration, if protection from disclosure is required, as the rest of the investigation.

The definition is, however, limited by the reference to a *penalty or sanction*.

A *penalty or sanction* would include a fine, imprisonment, revocation of a licence, an order to cease an activity, expulsion, or job loss.

A body other than the one carrying out the investigation can apply the penalty or sanction. This includes a body such as the RCMP or another federal agency that is not a public body as defined in the *Act*. Corporate security investigations can lead to a police investigation or to laying of charges. Committees such as the Health Facilities Review Committee may make recommendations to a Minister who invokes the sanctions. One private contractor may carry out by-law or safety codes investigations for several municipalities.

To apply the law enforcement exception, public bodies will need to ensure that a specific authority to investigate is in place and that the investigation can lead to a penalty or sanction being imposed.

Three types of investigations are specifically included: police, security and administrative investigations.

A *police investigation* is one carried out by the police, or other persons who carry out a policing function that involves investigations. For example, a police investigation may include an investigation by a special constable appointed under the *Police Act*, or by an officer responsible for investigating possible offences under a federal or provincial enactment.

A *security investigation* includes an activity carried out by, for, or concerning a public body and relates to the security of the organization and its clients, staff, resources, or the public. Security includes the work that is done to secure, ensure safety or protect from danger, theft or damage. This role may be assigned to private-sector security companies in rented property, corporate security departments or security staff in a local public body. Examples include investigations of parking offences on private property, employee theft, unlawful access to computer systems, and trespass on public body property.

Investigations carried out by information technology staff as part of protecting the integrity of computer hardware and software may also be considered security investigations.

An *administrative investigation* is a formal investigation carried out to enforce compliance or to remedy non-compliance with standards, duties and responsibilities.

These standards, duties and responsibilities may be defined under an Act, regulation or by-law. Examples include municipal by-law investigations, fire investigations, investigations under the *Safety Codes Act* and investigations carried out by an Attendance Board under the *School Act*.

Because of the nature of administrative investigations, they may not always be specifically authorized in an Act, regulation or by-law. Standards, duties and responsibilities may be defined in a formal policy of the public body. The establishment of a policy demonstrates that the public body considers an issue to be of sufficient importance to warrant the use of investigative procedures and the establishment of a possible sanction or penalty. It also demonstrates endorsement of the procedure and sanction by the governing body or the head of the public body.

Such policies should be clear about:

- the authority for the investigation;
- the nature of the investigation and procedures that must be followed; and
- the nature of the penalty or sanction.

Examples of this type of investigation would include:

- an investigation in response to a complaint under a public body's sexual harassment policy;
- an investigation in accordance with a public body's policy on maintaining confidentiality of client, staff and organizational information; and
- an investigation pursuant to an educational body's procedures on dealing with allegations of cheating.

The regular day-to-day review and monitoring of employee performance, including employee grievances, would generally not be considered an administrative investigation that is defined as law enforcement.

A civil action for monetary damages or recovery of a debt, or an internal employment-related investigation where a tribunal could hear the matter only at the insistence of the employee, does not fall within this section.

Investigations performed under the authority of a federal or provincial Act or regulation which can result in a prosecution would generally be considered to be part of law enforcement. The specific facts of the matter would determine whether it was a police, security or administrative investigation.

Proceedings include an action or submission to any court, judge or other body having authority, by law or by consent, to make decisions concerning a person's rights. This includes administrative proceedings before agencies, boards and tribunals that lead or could lead to a penalty or sanction being imposed, including a penalty or sanction imposed by another body to which the results of the proceeding may be referred.

Section 19(1) is a discretionary exception. It provides that a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to:

- harm a law enforcement matter;
- prejudice the defence of Canada or of any foreign state allied to or associated with Canada, or harm the detection, prevention or suppression of espionage, sabotage or terrorism;
- harm the effectiveness of investigative techniques and procedures currently used, or likely to be used, in law enforcement;
- reveal the identity of a confidential source of law enforcement information;
- reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression of organized criminal activities or of serious and repetitive criminal activities;
- interfere with or harm an ongoing or unsolved law enforcement investigation, including a police investigation;

- reveal any information relating to prosecutorial discretion;
- deprive a person of the right to a fair trial or impartial adjudication;
- reveal a record that has been confiscated from a person by a peace officer in accordance with a law;
- facilitate the escape from custody of an individual who is being lawfully detained;
- facilitate the commission of an unlawful act or hamper the control of crime;
- reveal technical information relating to weapons or potential weapons;
- harm the security of any property or system, including a building, a vehicle, a computer system or a communications system; or
- reveal information in a correctional record supplied, explicitly or implicitly, in confidence.

Harm a Law Enforcement Matter (section 19(1)(a))

This provision permits a public body to refuse disclosure of information that may result in harm to law enforcement activities themselves.

Harm implies damage or detriment. The harm threshold is designed to protect law enforcement while preserving the public's right of access to some types of law enforcement information.

The public body needs to demonstrate that there is a reasonable likelihood of harm if specific information is disclosed. The likelihood of harm will depend, in part, on the sensitivity of the law enforcement information.

To invoke this exception, a public body must establish a direct link between the disclosure of specific law enforcement information and the harm that is expected to result from release. It cannot simply claim harm to law enforcement in general (see *IPC Order 96-003*).

A public body does not need to demonstrate that actual harm will result or that actual harm resulted from similar disclosures in the past. However, past experience is a valuable indicator of the expected harm.

Generally, this provision is used to protect law enforcement investigations that are active. It may also be used to protect the confidentiality of the process through which complaints are received.

Prejudice to the Defence of Canada (section 19(1)(b))

This provision allows a public body to refuse disclosure of information that could reasonably be expected to be detrimental to national security.

Public bodies in Alberta hold only limited information related to national security. However, the presence of military installations within the province and the need for cooperation between the federal and provincial governments for emergency planning are matters that could fall within the scope of this exception.

Prejudice in this context refers to detriment to national security interests.

Defence of Canada means any activity or plan relating to the defence of Canada, including improvements in the nation's ability to resist attack.

An *allied state* is one with which Canada has concluded formal alliances or treaties. An *associated state* is one with which Canada may be linked for trade or other purposes outside the scope of a formal alliance.

This provision also permits the public body to refuse disclosure of information that would harm the detection, prevention or suppression of espionage, sabotage or terrorism. The test for *harm* in this part of the exception is more demanding than the test for *prejudice* required in the first part. There must be clear and convincing evidence that harm to the detection, prevention or suppression of espionage, sabotage or terrorism could occur if the requested information were disclosed.

Espionage is any activity carried out by spies, or activity related to spying.

Sabotage is malicious or wanton destruction, usually, but not always, directed against property.

Terrorism involves acts of serious violence and related activities that create fear in individuals, groups or nations and which are generally aimed at coercing government or communities into taking or ceasing specific actions.

Examples include information relating to industrial sabotage or terrorism, such as bombings of oil field installations, and information concerning local security arrangements for a meeting of heads of state or an international sporting event.

Effectiveness of Investigative Techniques and Procedures (section 19(1)(c))

This provision permits a public body to refuse disclosure of information that could harm the effectiveness of investigative techniques used in law enforcement.

It recognizes that unrestricted access to law enforcement techniques could reduce their usefulness, proficiency and success (i.e., effectiveness).

Investigative techniques and procedures encompass the methods and processes by which examinations, inquiries and observations are carried out, and include the equipment and technology employed in these activities.

The harms test precludes the refusal of basic information about well-known investigative techniques such as wire-tapping, fingerprinting or standard sources of information about individuals' addresses, personal liabilities, real property, etc. (see *IPC Order 99-010*).

The focus in the exception is on the refusal of information that relates directly to the continued effectiveness of investigative techniques and procedures. Examples where less information might be disclosed are DNA testing or new technologies in electronic eavesdropping.

The exception extends to techniques and procedures *likely to be used*, in order to protect techniques and technology under development and new equipment or procedures that have not yet been used.

Identity of a Confidential Source (section 19(1)(d))

This provision enables a public body to refuse to disclose information that reveals the identity of a confidential source of law enforcement information. The fact that the information, if disclosed, could reveal the identity of a confidential source is sufficient to apply this exception. There is no need to actually demonstrate that harm could come to the source.

Identity includes the name and any identifying characteristics, symbols and numbers relating to the source.

A *confidential source* is someone who supplies law enforcement information, as defined in the *Act*, to a public body on the assurance that his or her identity will remain secret. Employees, whether directly employed or under contract, cannot be *sources* because they are a part of a public body and are supplying information as part of their job (see *IPC Order 99-010*).

Where a public body can demonstrate that the source is indeed confidential and is supplying law enforcement information, it then determines whether the particular information requested could possibly permit the applicant or anyone else to identify the source. Since it is often difficult to determine whether information can be linked to provide identification, caution should be exercised in releasing any information connected to a confidential source.

See also Police Informer Privilege in Chapter 4.14 of this publication. If police informer privilege applies, the information cannot be disclosed. This is a mandatory exception to disclosure because privileged information of a third party is involved (**section 26(2)**).

Reveal Criminal Intelligence (section 19(1)(d.1))

This provision allows a public body to refuse disclosure of information that could reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression of:

- organized criminal activities, or
- serious and repetitive criminal activities.

Criminal intelligence operations are related to policing activities but are mentioned separately to emphasize that they are covered in the exception. Criminal intelligence is information relating to a person or group of persons compiled by law enforcement agencies to anticipate, prevent or monitor possible criminal activity.

This exception does not require an expectation of harm. In order to qualify for this exception, the criminal intelligence must have a reasonable connection with operations relating to organized crime or with serious and repetitive criminal activities. A public body wishing to rely on this exception would have to be able to demonstrate a rational relationship between the information collected and the operations for which that information may be used.

Intelligence-gathering is often unrelated to the investigation of a specific offence. For example, intelligence may be used for future investigations, for activities aimed at preventing the commission of an offence, and for ensuring the security of individuals or organizations.

Intelligence may be drawn from investigations of previous incidents that may or may not have resulted in the trial and conviction of the person under surveillance.

Organized criminal activities occur when a group of people come together with the intent of committing crimes or when they conspire together to commit crimes. There is a degree of organization or deliberate planning involved, which is not the case with random criminal acts. Examples may include the activities of gangs and automobile theft rings, smuggling narcotics, and transporting illegal immigrants.

Serious and repetitive criminal activities occur when an individual, or group of individuals, commit the same crime repeatedly. The criminal activity has to be one that carries a heavy penalty or has major impact on society or individuals.

Examples include serial bank robberies, dealings in illegal drugs and ongoing industrial sabotage.

Interfere with or Harm a Law Enforcement Investigation (section 19(1)(d.2))

This provision allows a public body to refuse to disclose information that could either interfere with or harm an ongoing or unsolved investigation.

Interfere with is a less stringent test than the harms test under **section 19(1)(a)**. It includes hindering or hampering an investigation and anything that would detract from an investigator's ability to pursue the investigation.

The exception applies to ongoing or active investigations and those where investigative activity has ceased but the crime remains unsolved. This includes investigations where no prosecution has resulted, but not those where charges were dropped.

An example would be an unsolved murder or a fraud investigation where there was insufficient evidence for prosecution at the time of the investigation.

The public body must demonstrate the harm that would result from disclosure (see **section 19(1)(a)** above), or the way in which disclosure would interfere with or hinder the investigation.

Prosecutorial Discretion (section 19(1)(d.3))

This provision allows a public body to refuse to disclose information related to the exercise of discretion by Crown Counsel or a special prosecutor with regard to prosecuting an offence.

This includes information on whether or not to:

- approve a prosecution,
- stay a proceeding,
- prepare for a hearing or trial,
- conduct a hearing or trial,
- take a position on a sentence, or
- initiate an appeal.

The exercise of this discretion applies to offences under the *Criminal Code* (Canada) and any other enactment of Canada for which the Minister of Justice and Attorney General for Alberta may initiate and conduct a prosecution. It also extends to offences under an enactment of Alberta, including prosecution of provincial regulatory offences. Most records relating to this exception will be in the custody or under the control of Alberta Justice. Copies of records or notes reflecting the discretion exercised may be in the files of other public bodies, especially police services.

Section 19(1.1) states that this exception does not apply to information that has been in existence for 10 years or more. Normally this is determined by matching the day and month on the face of a record to the same day and month ten years later. Where the date is not obvious, it will be necessary to examine the context of the record, other documents that may be in proximity to it in a file and other facts that will help to provide a date.

Fair Trial or Impartial Adjudication (section 19(1)(e))

This provision enables a public body to refuse to disclose information that could reasonably be expected to deprive a person of the right to a fair trial or impartial adjudication. The exception applies to a person. *Person* includes an individual, a corporation, a partnership and the legal representatives of a person.

Fair trial refers to a hearing by an impartial and disinterested tribunal that renders judgment only after consideration of the evidence and the facts.

Impartial adjudication means a proceeding in which the parties' legal rights are safeguarded and respected.

It is important that discussions proceed and decisions on these matters continue to be made in a candid manner without any fear of interference from outside influences.

This exception applies beyond law enforcement and civil and criminal court actions to proceedings before tribunals established to adjudicate individual and collective rights. Examples include hearings before the Hospital Privileges Appeal Board, and the hearings of a human rights panel.

In applying the exception, the public body must present specific arguments about how and why disclosure of information could deprive a person of the right to a fair trial or hearing. Commencement of a legal action is not by itself enough to support application of this exception.

An example of a case where the exception might apply would be if there were a request for information about alleged sexual abuse collected as part of a case against an individual. Disclosure of such information before legal proceedings were completed could reasonably be expected to detract from an individual's right to a fair trial.

Confiscated Records (section 19(1)(f))

This provision permits a public body to refuse disclosure that would reveal a record that has been seized from a person by a peace officer in accordance with the law.

The provision covers individuals, corporations and partnerships, and their representatives.

A *peace officer* includes a mayor, sheriff or sheriff's officer, warden, correctional officer, and any other officer or employee of a penitentiary, prison or correctional centre. It also includes a police officer, police constable, special constable or other person employed for the preservation or maintenance of public peace.

The record must have been confiscated under the authority of a law or statute. An example would be business records of a company under investigation for suspected tax fraud where its records have been seized.

Facilitating Escape from Custody (section 19(1)(g))

This provision allows a public body to refuse disclosure of information where release could reasonably be expected to facilitate the escape from custody of a person who is lawfully detained.

Lawfully detained means being held in custody pursuant to a valid warrant or other authorized order. This would include:

- those in custody under federal or provincial statute;
- young persons in open or secure custody or pre-trial detention under the Alberta *Young Offenders Act*;
- those involuntarily committed to psychiatric institutions; and
- parole violators held under a warrant.

The exception also extends to individuals remanded in custody (i.e., charged but not yet found guilty and sentenced). It does not apply to individuals released under bail supervision. An example of information protected by this exception is the building plans for a correctional facility.

Facilitate the Commission of an Unlawful Act (section 19(1)(h))

This provision permits a public body to refuse to disclose information that would be of use in committing a crime or that could hamper the control of crime. Examples include information about techniques, tools and instruments used for criminal acts, names of individuals with permits for guns, the location of police officers, and the location of valuable assets belonging to a public body.

Reveal Technical Information Relating to Weapons (section 19(1)(i))

This provision enables a public body to refuse the disclosure of information that could reasonably be expected to make the applicant or others aware of technical information relating to weapons or to materials that have the potential to become weapons. This exception would cover information such as how to make a bomb.

Security of Property and Systems (section 19(1)(j))

This provision permits the public body to refuse to disclose information that could reasonably be expected to harm the security of any property or system, including a building, a vehicle, a computer system, and a communications system. The same rules for determining harm apply as to other parts of **section 19** where there is a harms test.

Security generally means a state of safety or physical integrity. The security of a building includes the safety of its inhabitants or occupants when they are present in it. Examples of information relating to security include methods of transporting or collecting cash in a transit system, plans for security systems in a building, patrol timetables or patterns for security personnel, or the access control mechanisms and configuration of a computer system.

Correctional Record (section 19(1)(k))

This provision enables a public body to refuse to disclose all or part of a record that could reasonably be expected to reveal information in a correctional record supplied explicitly or implicitly in confidence.

A *correctional record* refers to information collected or compiled while an individual, either an adult or young person, is in the custody or under the supervision of correctional authorities or their agents as a result of legally imposed restrictions. It includes records relating to:

- imprisonment,
- parole,
- probation,
- community service orders,
- bail supervision, and
- temporary absence permits.

The record itself need not be in the custody or control of the public body. It will suffice if the information would reveal information that is in the correctional record. The information may be an extract from the record or a summary of the record.

To qualify for the exception, the information must have been supplied in confidence. This means that there is an agreement or understanding between the parties or some long-standing practice governing how the information will be treated. This may be explicit, in that it has been agreed to in writing, or implicit, in that both parties assume the confidentiality.

It is not sufficient to simply mark the information as being received in confidence. There must be evidence that a condition of confidentiality is a normal part of the process of supplying the information. For more information on the confidentiality, see section 4.3 of this chapter.

Section 19(2) is also a discretionary exception. It allows non-disclosure of information that could expose an individual to civil liability or could harm the proper custody or supervision of an individual under correctional supervision.

Exposure to Civil Liability (section 19(2)(a))

Section 19(2)(a) allows a public body to refuse to disclose information to an applicant if the information is in a law enforcement record and the disclosure could reasonably be expected to expose an individual to civil liability. To qualify for this exception, the individual must either be the author of the record, or be quoted or paraphrased in the record.

This exception protects law enforcement officials, and those providing information to them, from civil suit as a result of disclosure of records made while carrying out law enforcement activities.

Individual under the Supervision of Correctional Authority (section 19(2)(b))

Section 19(2)(b) allows a public body to refuse disclosure of information about the history, supervision or release of a person who is in custody or under the supervision of a correctional authority. The exception applies only if disclosure could reasonably be expected to harm the proper custody or supervision of that person. The same harms test is required as for **section 19(1)(a)**.

History means information about the person such as an employment record or medical information. *Supervision* refers to the overseeing of a person. The provision applies to adults and young persons still subject to control by correctional authorities or their agents as a result of legally imposed restrictions on their liberty.

This includes individuals in prison, on parole, on probation, on a temporary absence permit, under bail supervision or performing community service work. The exception allows discretion to except specific information about someone in custody or under supervision.

Examples include security arrangements for the transfer of a prisoner between facilities, whether or not a prisoner is in a public hospital, and the appointment of a probation officer.

This exception cannot be used to deny access to an applicant who is no longer in custody and is seeking his or her own personal information.

Offence under Act of Canada (section 19(3))

Section 19(3) is a mandatory exception. It provides that a public body must refuse to disclose information to an applicant if the information is a law enforcement record and the disclosure would be an offence under an Act of Canada.

Law enforcement record means any recorded information relating to law enforcement as defined in the *Act*.

An *offence under an Act of Canada* means a breach of a federal statute. It excludes lesser instruments such as federal regulations, orders or rules.

Examples of such legislation are:

- the *Young Offenders Act* (Canada), where it is an offence to knowingly disclose certain court, police, government and other records relating to young offenders except as authorized by that Act,
- the *Official Secrets Act* (Canada), which prohibits disclosure of information that could prejudice the security of the country, and
- the *Criminal Code* (Canada), which prohibits the release of wiretap transcripts.

When the Exception Does Not Apply (section 19(4))

Section 19(4) of the *Act* provides that **section 19(1)** and **section 19(2)** do not apply to:

- a report prepared in the course of routine inspections by an agency that is authorized to enforce compliance with an Act of Alberta (**section 19(4)(a)**); or
- a report, including statistical analysis, on the degree of success achieved in a law enforcement program, unless disclosure of the report could reasonably be expected to interfere with or harm the matters referred to in **section 19(1)** or **(2)**.

The intent is to encourage disclosure of reports and statistics about law enforcement programs.

Routine inspections involve periodic visits by public officials to ensure that standards or other criteria are being met. They take place without specific allegations or complaints having been made. Examples include inspections under the *Safety Codes Act*, public health inspections, fire inspections, liquor licensing inspections, and safety inspections on trucks or school buses.

Such reports are usually factual in nature and report the conditions found by the inspector. They may include advice or other information that could be excepted under other sections of the *Act*.

Reports and statistics on the success of law enforcement programs should also be routinely disclosed whenever possible. Only if the contents of the report could interfere with or harm any of the matters set out in the preceding sections would information be withheld, and this would be done by severing the appropriate parts of the report.

Examples include information on programs such as "Crimestoppers" and "Check Stop," statistics on elevator safety inspections, and reports on matters such as success in preventing abuse of handicapped parking stalls.

Completed Investigations (section 19(5))

Section 19(5) of the *Act* provides that, after a police investigation is completed, a public body may disclose the reasons for the decision not to prosecute:

- to a person who knew of and was significantly interested in the investigation, including a victim or a relative or friend of a victim (**section 19(5)(a)**); or
- to any other member of the public, if the fact of the investigation was made public (**section 19(5)(b)**).

This disclosure would be in response to a request for access to information under the *Act*. Disclosure of the decision not to prosecute is permitted only to persons who knew of *and* were significantly interested in the investigation, unless the fact of the investigation itself is public knowledge.

There is no general requirement to release information about decisions not to prosecute unless the investigation itself was made public. To apply **section 19(5)(b)** there would have to be evidence of this fact, such as a newspaper report about the investigation or a news release.

The provision relates only to police investigations and not to the whole field of law enforcement.

Existence of Record

There are situations in which the disclosure of the mere existence of a record could result in harm to law enforcement. For example, disclosure of the existence of investigation records or criminal intelligence may indicate that enforcement activities are being undertaken and this, in itself, could harm those activities.

Section 11(2)(a) of the *Act* provides that a public body may, in response to an applicant, refuse to confirm or deny the existence of a record containing information described in **section 19**.

When the existence of a record is neither confirmed nor denied, the response to the applicant, as required under section 11(1) of the *Act*, must incorporate a statement as provided for in Model Letter I in Appendix 3 of this publication.

The same conditions apply as outlined in section 4.4 of this chapter.

Application of Exception

Figure 5 contains a flowchart setting out the application of **section 19**.

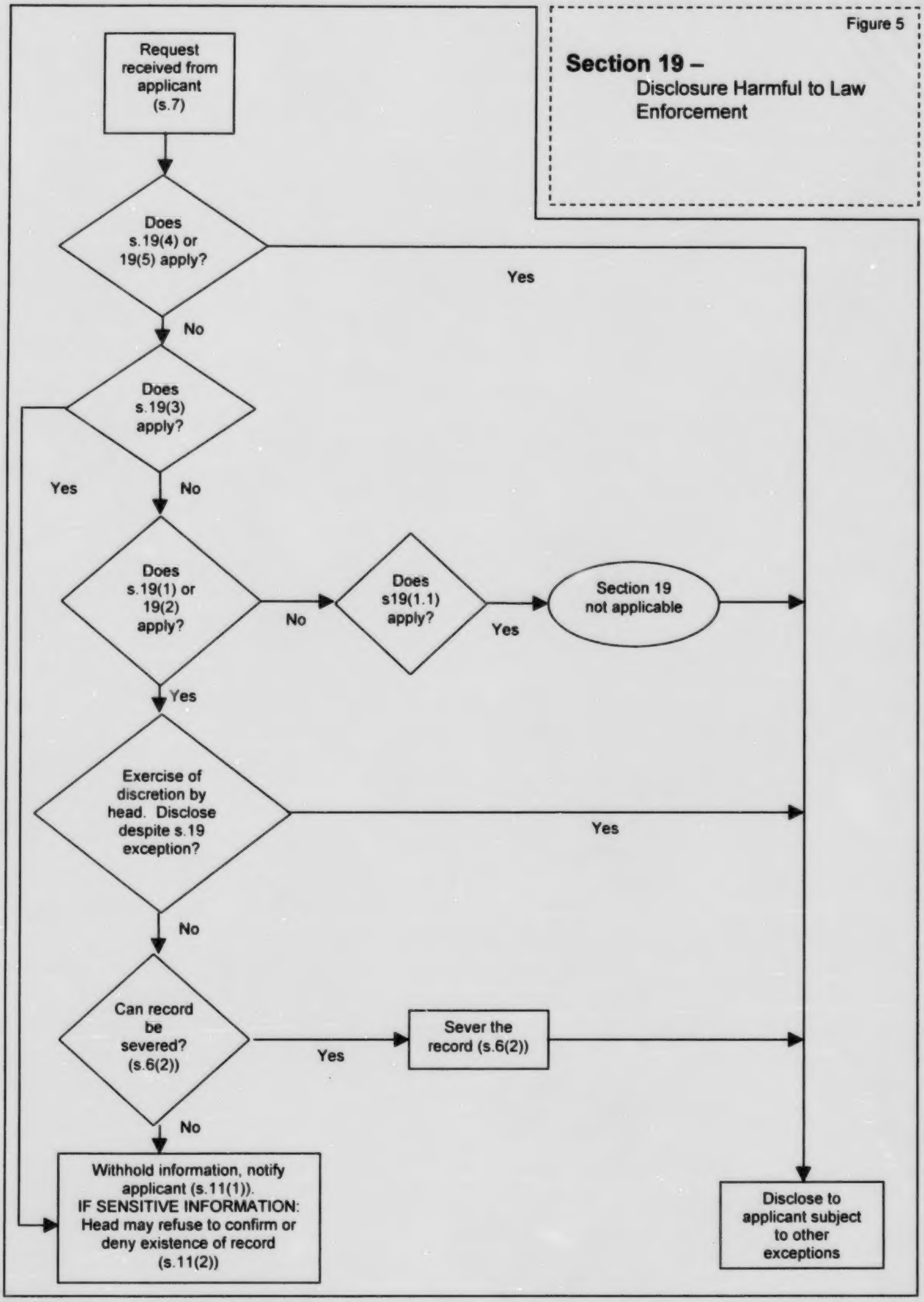


Figure 5

Section 19 –
Disclosure Harmful to Law Enforcement

Request received from applicant (s.7)
Does s.19(4) or 19(5) apply?
Yes
No
Does s.19(3) apply?
Yes
No
Does s.19(1) or 19(2) apply?
No
Does s19(1.1) apply?
Yes
Section 19 not applicable
Yes
Exercise of discretion by head. Disclose despite s.19 exception?
Yes
No
Can record be severed? (s.6(2))
Yes
Sever the record (s.6(2))
No
Withhold information, notify applicant (s.11(1)).
IF SENSITIVE INFORMATION: Head may refuse to confirm or deny existence of record (s.11(2))
Disclose to applicant subject to other exceptions

4.8 INTERGOVERNMENTAL RELATIONS

Overview

Section 20 provides that a public body may refuse to disclose information that could harm intergovernmental relations or the intergovernmental supply of information.

Section 20 is a discretionary exception.

Section 20(1) allows a public body to refuse access if disclosure could reasonably be expected to:

- harm relations between the Government of Alberta or its agencies and any of the following or their agencies:
  - the Government of Canada or a province or territory of Canada,
  - a local government body, as defined in the *FOIP Act* (see Chapter 1.2 of this publication),
  - an aboriginal organization that exercises government functions,
  - the government of a foreign state, or
  - an international organization of states,

  or
- reveal information supplied explicitly or implicitly in confidence by a government, local government body or an organization listed above or its agencies.

This exception has two parts, one dealing with *harm to relations* and the other with *information given in confidence.*

Harm to Relations (section 20(1)(a))

This provision applies to information the disclosure of which could reasonably be expected to harm relations between the Government of Alberta and the listed external government entities. It includes both current and future relations.

Relations is intended to cover both formal negotiations and more general exchanges and associations between the Government of Alberta and other governments and their agencies.

Harm means damage or detriment to negotiations and general associations and exchanges. The threshold of harm is relatively high. To satisfy the test there must be more substantial grounds than fear that disclosure would merely hinder, impede or minimally interfere with the conduct of intergovernmental relations or negotiations.

The term *Government of Alberta* connotes a broader sense here than that of an individual provincial public body. The exception has a different and higher-level coverage, in that *government* is intended to convey the sovereign power of the state in carrying out its will and functions. The exception is available only where disclosure of information could harm the conduct of intergovernmental relations of the province as a government entity, as opposed to interdepartmental relations.

Public bodies wishing to invoke **section 20(1)(a)** must demonstrate that the conduct of intergovernmental relations of the Government of Alberta, and not just those of the public body, would be harmed by disclosure.

The exception relates to government bodies external to the Government of Alberta, to certain aboriginal organizations and to local government bodies.

It also covers any of their agencies (i.e., corporate bodies or persons designated by any of the listed external government organizations).

For example, the Department of National Defence is an agency of the Government of Canada, UNESCO is an agency of the United Nations, and an economic development agency is an agency of a local government.

The provision covers not only *provincial governments* but also *territorial governments* (e.g., the Government of the Yukon) and their agencies.

An *aboriginal organization* refers to the council of a band as defined in the *Indian Act* (Canada) and any organization established to negotiate or implement, on behalf of aboriginal people, a treaty or land claim with the federal government. This definition in relation to treaties and land claims does not limit the subject matter of the records to which the exception may apply. The particular records need not deal with treaties or land claims.

A *foreign state* refers to the government of any foreign nation or state, including the component state governments of federated states.

An *international organization of states* refers to any organization with members representing and acting under the authority of the governments of two or more states. Examples would be the United Nations or the International Monetary Fund.

Examples of information that might qualify for this exemption include:

- correspondence between the Department of Human Resources and Employment and the International Labour Organization regarding employment standards, where disclosure might severely damage the ability of the Government of Alberta and this international body to carry on negotiations; and
- notes of private discussions between officials of a city, its twinned counterpart in a developing country, the province and the country concerned, where no agreement has been reached between the parties to make the discussions public.

Disclosure of Information

Section 20(2) of the *Act* stipulates that information referred to in **section 20 (1)(a)** may only be disclosed with the consent of the Minister responsible for the *FOIP Act* (i.e., the Minister of Municipal Affairs) in consultation with the Executive Council.

Where a public body wishes to disclose information that qualifies for the exception set out in section 20 (1)(a), it must prepare a submission describing the information and setting out the circumstances and reasons why it wishes to disclose this information.

The submission should be prepared in consultation with either:

- **the Department of International and Intergovernmental Relations, where records concerning the federal, foreign governments, international organizations or aboriginal organizations are involved; or**
- **the Department of Municipal Affairs or other relevant department, where local governments are involved,**

and with the other government, as appropriate.

This submission must then be signed by the head of the public body and submitted to the Minister of Municipal Affairs for consideration.

If, after discussion of the matter with the public body and with other appropriate departments, the Minister of Municipal Affairs believes that disclosure should take place, the Minister and the head of the relevant Alberta Government department will jointly sponsor the submission to the Executive Council for consultation.

After this consultation, the Minister will either consent to, or deny, the application.

Information Received In Confidence (section 20(1)(b))

This section provides protection for information that could reasonably be expected to reveal information received in confidence from one of the bodies specified in **section 20(1)(a)**.

A decision that a confidence would be revealed is enough to satisfy the test here. It is *not* necessary that the harms test set out in **section 20 (1)(a)** also be met.

In order to be covered by **section 20(1)(b)**, the information must have been supplied in circumstances that clearly place an obligation on the public body to maintain confidentiality.

In confidence usually describes a situation of mutual trust in which private matters are related or reported.

Criteria for determining whether information has been given *in confidence* are provided in section 4.2 of this chapter.

The burden of determining that information was submitted *in confidence* lies with the public body.

The intention to maintain confidentiality may be explicitly stated within the record itself, or in an agreement between the parties, or may be implied by the circumstances under which the information was submitted and received. Where confidentiality is implied, there must be objective grounds to support the assumption of confidentiality. It is not sufficient for an external governmental entity to stamp documents "Confidential" or to assert that the information was supplied in confidence, although this will assist in the determination.

There must be evidence to support the assertion and to prove that the information has been treated consistently in a confidential manner.

Examples of information that may be supplied in confidence include:

- information exchanged between the Canadian Security Intelligence Service and municipal police forces;
- correspondence about and transcripts of a confidential meeting of the western Premiers; and
- negotiating strategies relating to a federal, provincial and municipal infrastructure program.

***Consent to disclose*: Section 20(3)** of the *Act* provides that a public body may disclose information supplied in confidence only with the consent of the government (provincial, territorial or foreign), the local government body, the organization or the agency that supplied the information.

Consultation with the other party or parties providing the information should take place between officials who are authorized to make decisions about disclosure. The consent of the government, local government body, organization or agency that provided the information should be in writing.

Limitation on Section 20 (section 20(4))

This provision states that **section 20** does not apply to information that has been in existence in a record for 15 years or more.

Normally, this is determined by matching the day and month on the face of a record to the same day and month 15 years later. Where the date is not obvious, it will be necessary to examine the context of the record, other documents that may be in proximity to it in a file and other facts that will help provide a date.

Information qualifying for exception under **section 20** but which is 15 or more years old must be released unless another exception applies to it.

Consultation

Consultations regarding whether or not to invoke this exception should normally take place between the FOIP Coordinator of the public body and officials in comparable positions in external government bodies.

Where the federal or foreign governments, aboriginal organizations or international organizations are involved, consultations must be conducted in cooperation with the Department of International and Intergovernmental Relations.

Where local governments are involved, consultation would occur with the appropriate public body, as indicated by the nature of the records.

Public bodies that will need to consult on a regular basis should establish practices and contact points to expedite the process

Application of Exception

Figure 6 contains a flowchart setting out the application of **section 20**.

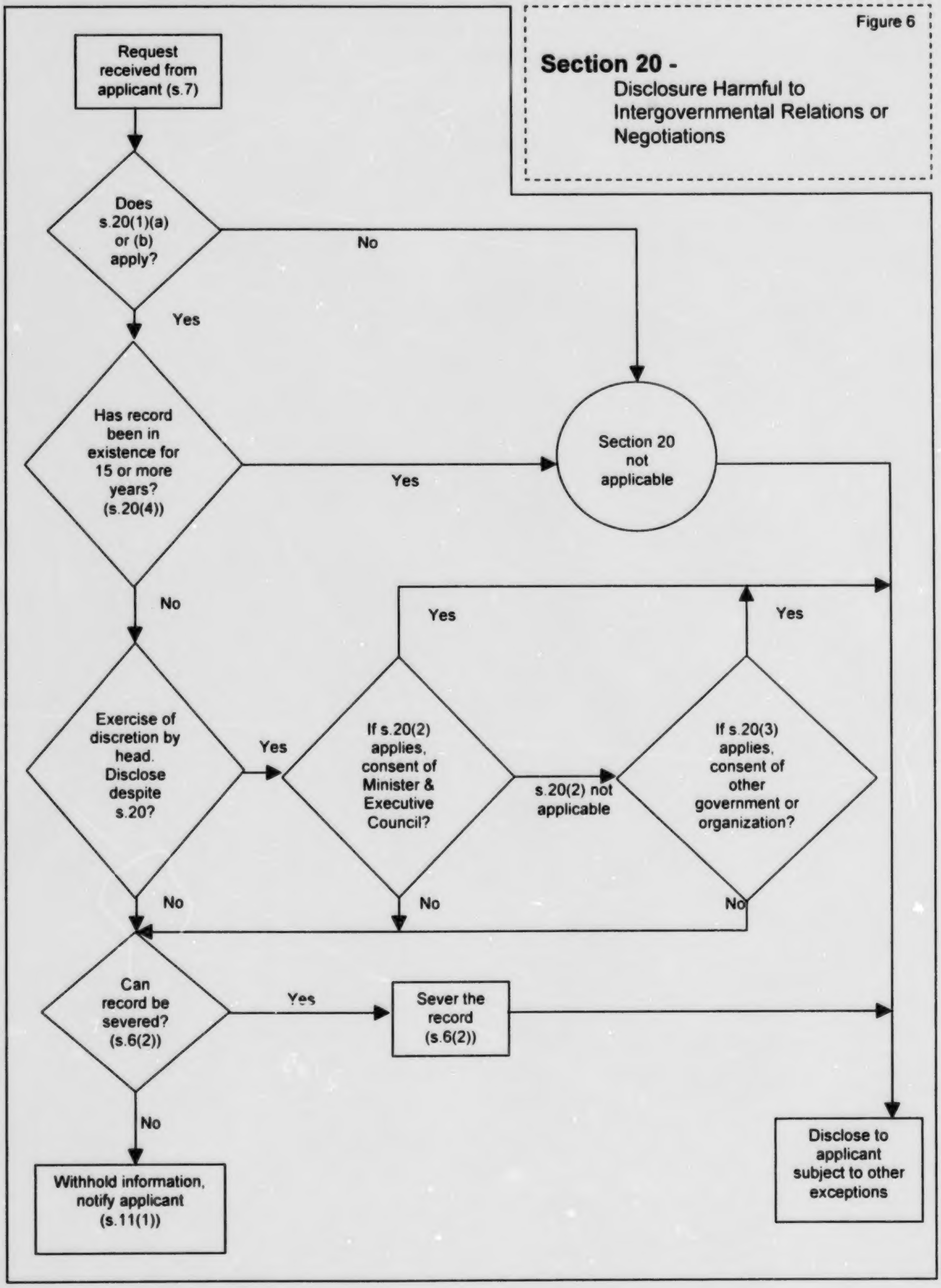

Request received from applicant (s.7)
Does s.20(1)(a) or (b) apply?
No
Yes
Has record been in existence for 15 or more years? (s.20(4))
Yes
Section 20 not applicable
No
Yes
Yes
Exercise of discretion by head. Disclose despite s.20?
Yes
If s.20(2) applies, consent of Minister & Executive Council?
s.20(2) not applicable
If s.20(3) applies, consent of other government or organization?
No
No
No
Can record be severed? (s.6(2))
Yes
Sever the record (s.6(2))
No
Withhold information, notify applicant (s.11(1))
Disclose to applicant subject to other exceptions

Figure 6

Section 20 -
Disclosure Harmful to Intergovernmental Relations or Negotiations

4.9 CABINET AND TREASURY BOARD CONFIDENCES

Overview

Section 21(1) creates a mandatory exception for information that would reveal the substance of deliberations of the Executive Council or any of its committees. It also applies to the Treasury Board or any of its committees. The exception applies to any advice, recommendations, policy considerations or draft legislation or regulations submitted to or prepared for submission to these bodies.

Section 21(1) is intended to preserve the unique role of Cabinet institutions and conventions within the framework of parliamentary government in Alberta. This is based on the convention of collective ministerial responsibility to the Legislature and the people of the province for the actions of the government.

In practice, all members of a Cabinet are expected to publicly support the government's actions and policies. In order to facilitate this collective decision-making, Cabinet discussions and deliberations have traditionally been kept confidential. This permits full and frank discussions around the Cabinet table. Ongoing confidentiality is required in order to avoid breaking a position of unity once a decision has been made.

In addition, there are situations where Cabinet may wish to delay public announcement of its decisions. It may have entered into arrangements with other governments or with affected individuals to postpone an announcement of a decision until a specific time.

Cabinet may also develop plans to deal with issues, emergencies or contingencies. The value of these plans would be diminished if immediate access were granted to its decision-making processes.

Standing Policy Committees (SPCs) are not considered Cabinet committees. It is recognized that information often flows among Cabinet, Treasury Board and SPCs and it is often difficult to distinguish the origins and purpose of particular information. In dealing with SPC records, or records created for SPCs, **sections 21, 23** (advice and recommendations) and **4(1)(l)** (which excludes some SPC information from the scope of the *Act*) must be applied in concert with each other.

Because **section 21** deals with the Cabinet process, the Office of the Executive Council makes all decisions relating to submissions to the Executive Council and related records (e.g., minutes and agendas). Treasury makes all decisions relating to submissions to Treasury Board and related records.

Departmental decisions on disclosure of other records that include reference to Cabinet or Treasury Board confidences are subject to approval by the Office of the Executive Council and Treasury respectively.

In the case of records containing Treasury Board confidences, the approval requirement relates only to records that are part of the Treasury Board decision-making process. It does not extend to records that Treasury Board requires departments to prepare, such as business plans. These are departmental operational records.

Consultation on confidences of the Executive Council must be conducted through the office of the FOIP Coordinator, Office of the Executive Council. Consultation on confidences of Treasury Board must be conducted through the FOIP Coordinator, Treasury.

Substance of Deliberations

In considering this exception, it is important to determine whether or not a record or part of a record reveals the substance of the deliberations of the Executive Council, the Treasury Board or any of their committees, either explicitly or implicitly.

A release of information *explicitly* reveals the substance of deliberations if the information itself contains the essence of the discussion or deliberations or reveals the contents of the deliberations.

A release of information *implicitly* reveals this type of information if it is reasonable to expect that disclosed information could be combined with other information to reveal the substance of Executive Council, Treasury Board or committee deliberations.

In this provision, *substance* means the essence or essential part of a deliberation.

Deliberation means the act of weighing and examining the reasons for and against a contemplated act or course of conduct. It also includes an examination of choices of direction or means to accomplish an objective.

Meaning of Executive Council

The Executive Council is commonly known as the provincial Cabinet and refers to a group of ministers acting collectively. **Section 21(1)** does not apply to a minister acting alone, unless the individual minister is carrying out the direction of Cabinet or is acting as a Cabinet committee.

Committees of the Executive Council include the Agenda and Priorities Committee, standing committees and ad hoc committees struck to deal with specific issues.

Committees of the Treasury Board refers to similar committees.

Examples of Records

Examples of records that would reveal the substance of deliberations of the Executive Council, Treasury Board or one of their committees are:

- agendas, minutes and related documents of Executive Council meetings;
- letters and memoranda concerning issues deliberated upon or the decisions or directions taken by ministers but not made public – these

may have been sent to ministerial colleagues or senior public servants;
- briefing material, exclusive of background facts, placed before Executive Council, Treasury Board or one of their committees;
- a memorandum (including electronic mail) from the Secretary to Cabinet to ministers discussing Cabinet decisions;
- a memorandum (including electronic mail) from a deputy minister to an assistant deputy minister or chief executive officer or other senior officer dealing with issues that will be or have been deliberated upon by the Executive Council, Treasury Board or one of their committees;
- a record of discussions between senior officials about issues that will be or have been deliberated upon by the Executive Council, Treasury Board or one of their committees;
- a briefing note from a deputy minister or chief executive officer to a minister concerning what will be, is or has been discussed in Executive Council, Treasury Board or one of their committees; and
- a draft or final submission to Executive Council or Treasury Board, excluding background facts.

The listing of types of records included in **section 21(1)** (advice, recommendations, policy considerations, and draft legislation or regulations) is illustrative only. These are simply examples of certain types of information likely to reveal deliberations of the Executive Council, Treasury Board or their committees.

Advice, recommendations refers to the substance of a suggested course of action which is the subject of deliberation. Advice is analysis and presentation of various options and not the presentation of fact. To qualify for this exception it must deal with issues that will be, are or have been discussed by the Executive Council, the Treasury Board or one of the committees of either body.

Policy considerations refers to analysis and flagging of issues that deserve special consideration by ministers when taking action or deciding policy at Executive Council, Treasury Board or a committee of either.

Draft legislation or regulations refers to versions of bills intended to become Acts or of legislative instruments intended to be enacted under the authority of an Act or the authority of the Lieutenant Governor in Council. This provision relates to draft legislation or regulations discussed by ministers.

When the Exception Does Not Apply

Section 21(2) sets out various circumstances where **section 21(1)** does not apply.

***Information in a record that has been in existence for 15 years or more* (section 21(2)(a)):** The exception in **section 21(1)** applies only to records or portions of records that have been in existence less than 15 years. Other exceptions may apply to particular information in these records.

15 years means the period from a particular month and day to a corresponding month and day 15 years later.

Information in a record of a decision made by the Executive Council or any of its committees on an appeal under an Act **(section 21(2)(b)):** Where the Executive Council or one of its committees functions as an appeal body under an Act and makes a decision, the decision and any recorded reasons for the decision are available to the public.

Other portions of the record, such as the advice and recommendations supporting the deliberative process leading to a decision, remain subject to **section 21(1)**.

Background facts **(section 21(2)(c)):** Information in a record does not qualify for this exception if its purpose is to present background facts to the Executive Council, to the Treasury Board, or to any of the committees of either body, for consideration in making a decision and if:

- the decision has been made public;
- the decision has been implemented; or
- five years or more have passed since the decision was made or considered.

This provision permits the release of information prepared specifically with the intent of presenting factual information (i.e., explanations of situations, as opposed to advice, recommendations, or policy considerations or analysis) to the Executive Council, Treasury Board or any of their committees.

Background facts means facts that provide explanatory or contributory information or circumstances. Background facts are usually found in attachments to submission documents and are intended to assist Cabinet in its deliberations.

Information that would reveal the substance of deliberations of the Executive Council, the Treasury Board, or any of their committees, such as summaries of background materials that highlight issues and key implications for deliberations, would not constitute *background facts* for the purposes of this provision. This information remains subject to **section 21(1)**.

Section 21(2)(c) does not allow public bodies to except background facts from disclosure if one of three criteria apply.

First, the exception for Cabinet and Treasury Board confidences does not apply to background facts *if the decision has been made public*.

A decision *has been made public* if it has been communicated to the public in an authorized way. Communication to the public in an authorized way would include communication in a statement by a minister, a statement or release by a communications officer, a statement in Question Period, a presentation in the Legislative Assembly, or a letter or statement to the media.

A "leak" of information is not considered an authorized disclosure of information.

The exception for Cabinet and Treasury Board confidences also does not apply to information providing background facts *if the decision has been implemented.*

A decision *has been implemented* if the decision has been put into effect. A decision may not be considered to have been implemented if the decision remains subject to approval or is not final. A decision has been implemented if it has been acted upon, even if action with respect to the subject of the decision is not complete.

For example, if the Treasury Board decided to go forward with a government-wide spending cut, implementation would commence when a plan of action was communicated to departments. At that time, the background facts would cease to be protected by **section 21(1)**.

In cases where decisions are reconsidered, clarified, amended, reversed or delayed, the exception does not apply to background facts if the decision that has subsequently been reconsidered has either been made public or implemented. However, other provisions of the *Act* may prevent disclosure.

The Commissioner has noted that, in applying **section 21(c)**, it is necessary to examine the *context* in which a record containing background facts was presented to Cabinet. The fact that a decision on a particular subject has been made public does not mean that background facts respecting a *related* decision can be disclosed. One must consider precisely what decision was being deliberated when the background facts were submitted to Cabinet (see *IPC Order 97-010*).

Finally, the exception for Cabinet and Treasury Board confidences does not apply to background facts *if 5 or more years have passed since the decision was made or considered.*

5 years means from a particular month and day to a corresponding month and day 5 years later. This condition applies regardless of whether or not a decision has been made public or has been implemented.

If the background facts were presented to the Executive Council, Treasury Board or any of their committees for consideration in making a decision, and 5 years have elapsed, the exception to disclosure for the background information under **section 21(1)** does not apply.

Application of Exception

Figure 7 contains a flowchart setting out the application of **section 21.**

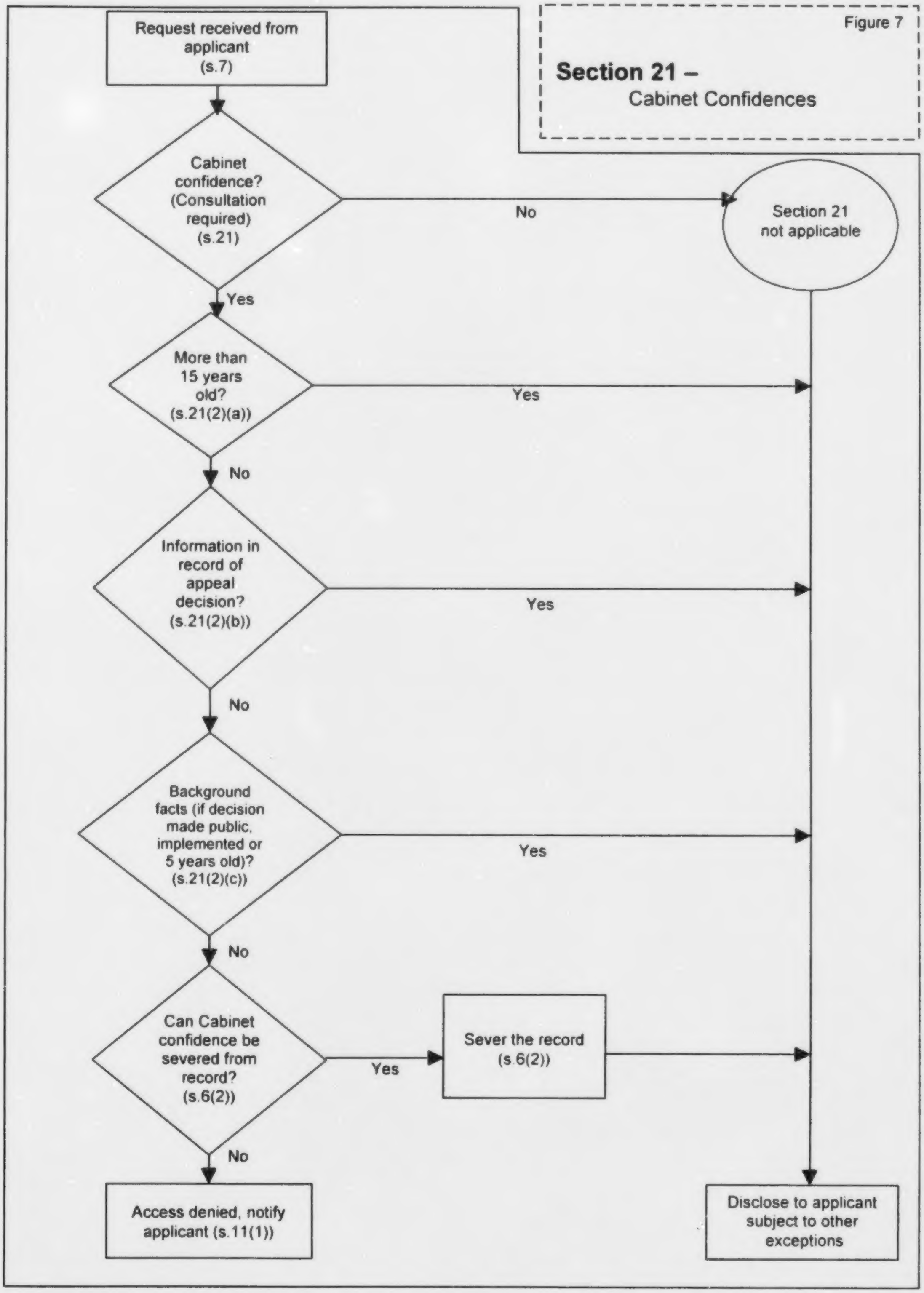


Figure 7

Section 21 – Cabinet Confidences

Request received from applicant (s.7)
Cabinet confidence? (Consultation required) (s.21)
No
Section 21 not applicable
Yes
More than 15 years old? (s.21(2)(a))
Yes
No
Information in record of appeal decision? (s.21(2)(b))
Yes
No
Background facts (if decision made public, implemented or 5 years old)? (s.21(2)(c))
Yes
No
Can Cabinet confidence be severed from record? (s.6(2))
Yes
Sever the record (s.6(2))
No
Access denied, notify applicant (s.11(1))
Disclose to applicant subject to other exceptions

4.10 LOCAL PUBLIC BODY CONFIDENCES

Overview

Section 22(1) of the *Act* provides that a local public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to reveal:

- a draft of a resolution, by-law or other legal instrument by which the local public body acts; or
- the substance of deliberations of a meeting of its elected officials or governing body or a committee of its governing body, if an Act or a regulation under the *FOIP Act* authorizes the holding of that meeting in the absence of the public.

Section 22 is a discretionary exception.

The provision refers to information, not records, which means that the exception should be applied only to that portion of a record containing information covered by this provision. The remainder of the severed record would be disclosed to the applicant unless another exception was invoked.

For example, an applicant requests a copy of a memorandum sent by the chair of a committee of a college board to committee members. The memorandum discusses a number of administrative matters and also discusses an issue that the committee must discuss at a forthcoming meeting that will not be open to the public. The information relating to this latter issue may be severed from the record if it would reveal the substance of deliberations of the committee on a matter specified in the FOIP Regulation or in another Act as one that may be considered *in camera*. The applicant would receive the remainder of the record unless other exceptions applied to it.

Draft Resolution, By-law or Other Legal Instrument

Draft means a version of the resolution, by-law or other legal instrument that has not been finalized for consideration in public by the local public body. The exception can apply to the whole draft record or to individual sections or clauses.

An example would be a preliminary version of a land use by-law drafted by a staff member for the consideration of a municipal council.

A *resolution* means a formal expression of opinion or will of an official body or public assembly, adopted by a vote of those present. The term is usually employed to denote the adoption of a motion such as an expression of opinion, a change to rules or a vote of support or censure. Most local public bodies take action by resolution.

For example, an official of a school district drafts a resolution setting out amended rules for the operation of individual schools. This amendment to the rules goes through several internal drafts before it is presented to the school board for discussion and consideration for approval. All versions other than the version that is submitted to the board may be withheld under this provision.

A *by-law* means a rule adopted by a local public body with by-law making powers.

Other legal instrument by which a local public body acts is a "catch-all" phrase to cover any other legal or formal written documents, other than resolutions or by-laws, which relate to the internal governance of a local public body or the regulation of the activities over which it has jurisdiction.

The intent of this provision is to extend to legal instruments of a local public body the same protection extended to provincial government legislation and regulations in **section 23(1)(e)**. Drafts are protected; the final version of the by-law, resolution or other legal instrument is not.

Substance of Deliberations of *In Camera* Meetings

In **section 22(1)(b)**, *substance* means the essence or essential part of discussion or deliberation.

Deliberation means the act of weighing and examining the reasons for and against a contemplated act or course of conduct. It also includes an examination of choices of direction or means to accomplish an objective.

Meeting means an assembly or gathering at which the business of the local public body is considered. It includes both the meeting in its entirety and a portion of a meeting.

Elected officials means those individuals publicly elected through a balloting process to conduct the business of the local public body.

Governing body means the assembly of persons who are responsible for the administration of the local public body.

Section 4(1.1) further defines this term, for the purposes of this section, in relation to post-secondary educational institutions as meaning:

- the board of governors or general faculties council of a university; or
- the board of governors or academic council of a college or technical institute.

Committee of its governing body means a group of people who have been designated by the governing body of the local public body to act on its behalf and consider a particular issue or subject. A committee may be composed of elected officials, members of the local public body or other persons designated to act by the local public body.

In order for information relating to a meeting held *in camera* to qualify for this exception, the holding of the meeting in the absence of the public must be authorized by:

- an Act of Alberta, not including any regulations, rules or by-laws made under that Act; or
- **section 18** of the FOIP Regulation, which specifies the conditions under which such meetings may be held and the subject matter that can be discussed.

If there is no specific provision relating to *in camera* meetings in the Act that establishes and governs a local public body, then information may be excepted from disclosure only if the subject matter considered in the absence of the public concerns, and is limited to:

- security of the property of the public body;
- personal information of an individual, including an employee of the public body;
- the acquisition or disposition of property by or for the public body;
- labour relations or employee negotiations;
- a law enforcement matter, litigation or potential litigation, including matters before administrative tribunals; or
- consideration of a request under the *FOIP Act* if the governing body or committee is itself designated as the head of the local public body.

A public body must rely on an authority as described above to authorize a meeting in the absence of the public and have grounds for excepting the substance of deliberations of such a meeting.

The provision in the FOIP Regulation applies to post-secondary educational bodies, which do not have provisions relating to *in camera* meetings in their governing legislation. It does not apply, for example, to public bodies subject to the *Municipal Government Act*, which has its own provision related to *in camera* meetings.

In the absence of the public means in the absence of the public at large. A meeting may still be considered to be held in the absence of the public if it is attended by a member of a local public body who is not an elected official, member of the governing body or member of a committee of the governing body.

A meeting open to the public, which no members of the public happen to attend, is not a meeting held in the absence of the public.

A meeting that is permitted to be held *in camera*, but to which the public is nevertheless invited, is also not a meeting held in the absence of the public.

However, a meeting, which may be held *in camera*, but to which certain members of the public are specifically invited to discuss sensitive issues pertaining to their property or themselves or their rights, is a meeting held in the absence of the public.

Common types of records relating to *in camera* meetings that may be protected are agendas, minutes, personal notes, and other records that document the substance of deliberations within such a meeting.

Actual documents that may be the subject of discussions, such as a report detailing an investigation into a complaint against a teacher, or a proposal from a company for tax concessions in return for a development project, could not normally be withheld under this section. However, the substance of deliberations about such documents may be withheld. This information will usually be part of other records and will have to be severed from them.

When the Exception Does Not Apply

The exception in **section 22(1)(a)** does not apply where the draft of the resolution, by-law or other legal instrument has been considered in a meeting open to the public. This means that, if a particular draft is discussed in a public meeting, there is no reason to deal with the information under an exception. Prior or subsequent drafts that are not considered in a public meeting can still be protected.

The exception in **section 22(1)(b)** does not apply where the subject matter of the deliberation has been considered in a meeting open to the public. This means that, where a local public body has not explicitly excluded the public from the meeting, the exception cannot be applied.

Finally, the exception cannot be applied to any information referred to in **section 22(1)(a)** and **(b)** if it is in a record that has been in existence for 15 years or more.

15 years means the period from a particular month and day to a corresponding month and day 15 years later. Other exceptions may still apply to the information.

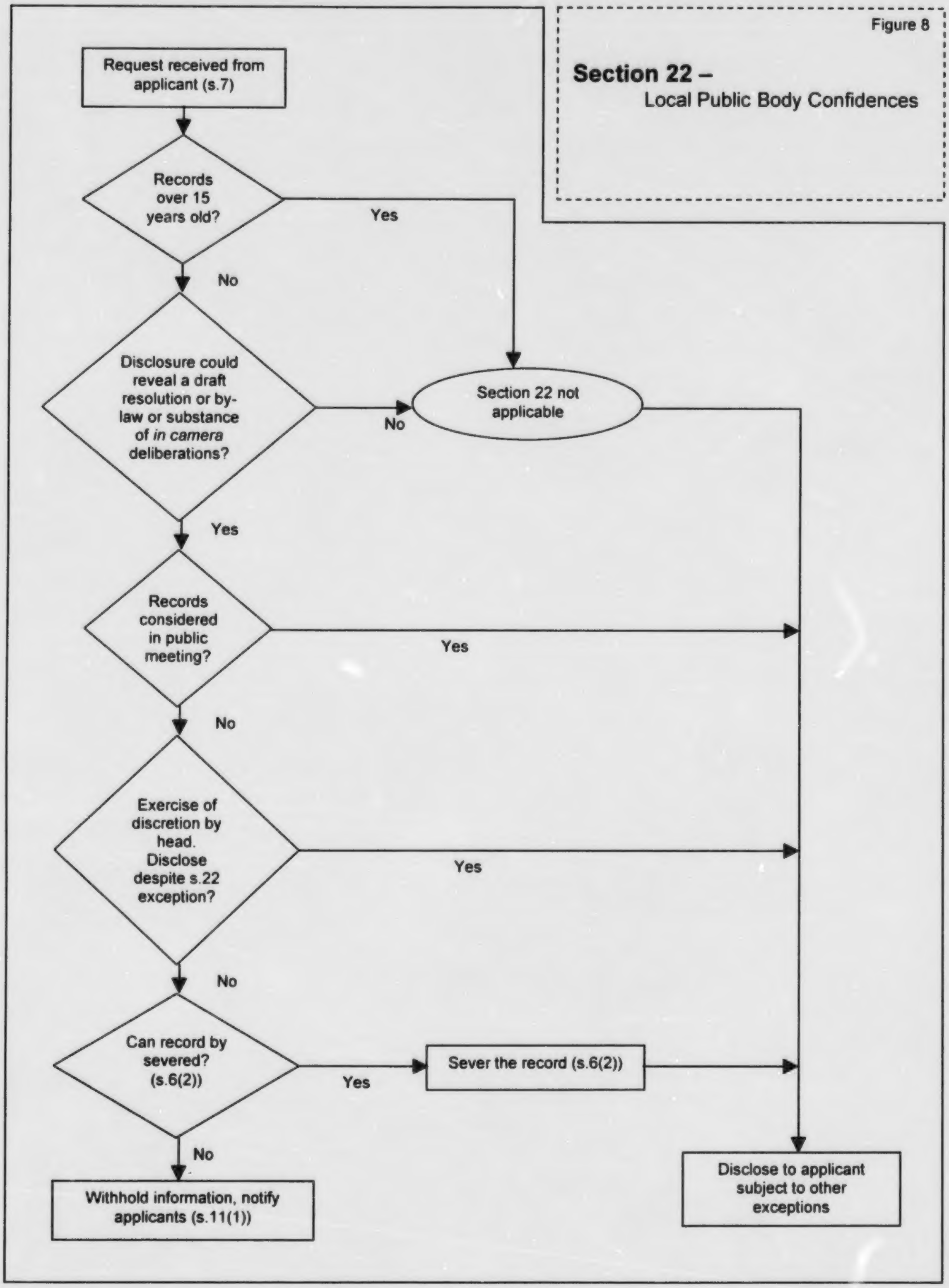
Application of Exception

Section 22 is applied in a series of steps that are outlined in the flowchart in ***Figure 8.***

Figure 8

Section 22 –

Local Public Body Confidences


Request received from applicant (s.7)
Records over 15 years old?
Yes
No
Disclosure could reveal a draft resolution or by-law or substance of *in camera* deliberations?
No
Section 22 not applicable
Yes
Records considered in public meeting?
Yes
No
Exercise of discretion by head. Disclose despite s.22 exception?
Yes
No
Can record by severed? (s.6(2))
Yes
Sever the record (s.6(2))
No
Withhold information, notify applicants (s.11(1))
Disclose to applicant subject to other exceptions

4.11 ADVICE FROM OFFICIALS

Overview

Section 23(1) provides that a public body may refuse to disclose information if the disclosure could reasonably be expected to reveal:

- advice, proposals, recommendations, analyses or policy options developed by or for a public body or a member of the Executive Council (**section 23(1)(a)**);
- consultations or deliberations involving:
  - officers or employees of a public body,
  - a member of the Executive Council, or
  - the staff of a member of the Executive Council (**section 23(1)(b)**);
- positions, plans, procedures, criteria or instructions developed for the purpose of contractual or other negotiations by or on behalf of the Government of Alberta or a public body, or considerations that relate to those negotiations (**section 23(1)(c)**);
- plans relating to the management of personnel or the administration of a public body that have yet to be implemented (**section 23(1)(d)**);
- the contents of draft legislation, regulations and orders of members of the Executive Council or the Lieutenant Governor in Council (**section 23(1)(e)**);
- the contents of agendas or minutes of meetings of an agency, board, commission, corporation, office or other body that is designated as a public body in the FOIP Regulation (**section 23(1)(f)**);
- information, including the proposed plans, policies or projects of a public body, the disclosure of which could reasonably be expected to result in disclosure of a pending policy or budgetary decision (**section 23(1)(g)**); or
- the contents of a formal research or audit report that is incomplete unless no progress has been made on the report for at least 3 years (**section 23(1)(h)**).

Section 23(1) is a discretionary exception that is intended to protect the deliberative process involving senior officials and heads of public bodies, and their staff, as well as among officials themselves. It also protects the deliberative process involving senior officials, heads of public bodies and the governing authorities of local public bodies.

The need for confidentiality in relation to various aspects of decision-making is not restricted to decisions by the Executive Council or the governing authorities of local public bodies. An absolute rule permitting public access to all records relating to policy formulation and decision-making processes in public bodies would impair the ability of such bodies to discharge their responsibilities in a manner consistent with the public interest.

The exception is intended to provide a "deliberative space" for those involved in providing advice, carrying on consultations and making recommendations, so that records may be written with candour and cover all options. This "deliberative space" is especially important for those involved in the policy-making process. There is a need to preserve the relationships between senior officials and those advising them as part of the overall accountability of public organizations.

Senior officials and heads of local public bodies may accept or reject the advice and recommendations of those advising them and they carry the responsibility of defending that decision.

The whole exception is discretionary in nature. Discretion is exercised in determining whether or not disclosure of a particular record or part of a record could reasonably be expected to reveal particular information about *either the process itself or the matters being discussed*.

In determining whether or not to invoke the exception, public bodies should undertake a three-step process. They should:

- **determine whether the information requested falls within one of the classes of information to which the exception to disclosure may apply;**
- **if it does, then determine whether or not disclosure of the information can reasonably be expected to *reveal* the particular class of information involved; and**
- **exercise discretion as to whether or not to disclose the record or part of the record based on whether or not disclosure would affect similar advisory processes in the future.**

The exercise of discretion regarding this type of advisory information should be based on the impact the disclosure can reasonably be expected to have on the public body's ability to carry out similar internal decision-making processes in the future.

Consideration should be given to whether disclosure of the information in this instance would:

- make advisory processes less candid and comprehensive;
- make consultations or deliberations less frank;
- hamper the policy-making process;
- destroy the ability of a public body or the government to develop and maintain strategies and tactics for present or future negotiations; or
- undermine the public body's ability to undertake personnel or administrative planning.

Such determinations can only be made on a case-by-case basis, bearing in mind the magnitude of the process involved, the procedures for decision-making that have been followed, and the sensitivity of the particular information.

Public bodies should take into account the effect disclosure would have on all steps of a decision-making process and not just the immediate interests regarding the particular information in question.

The test for the exception is met if deliberative information is explicitly revealed or if a record makes direct reference to the deliberative processes.

As well, release of information can reveal deliberative processes implicitly if it allows an accurate inference to be made about those processes.

Eight specific areas meriting consideration for protection are set out in the *Act*. Each of these is discussed in detail below.

Advice and Recommendations

Section 23(1)(a) is intended to protect candour in the giving of advice and formulation of proposals, analyses, policy options, recommendations, and related alternatives for potential courses of action.

It covers such advisory functions at all levels in a public body. It also applies to advice and recommendations obtained from outside the public body, including those received under a contractual or other advisory arrangement. The exception provides specific coverage for advice, proposals, recommendations, analyses, and policy options developed by or for a member of the Executive Council.

There is some overlap between the terms *advice* and *recommendations* as used in the exception.

The term *recommendations* refers to formal recommendations about courses of action to be followed which are usually specific in nature and are proposed mainly in connection with a particular decision being taken.

Advice, on the other hand, refers to less formal suggestions about particular approaches to take or courses of action to follow.

Proposals and *analyses or policy options* are closely related to advice and recommendations and refer to the concise setting out of the advantages and disadvantages of particular courses of actions.

The Information and Privacy Commissioner has defined all these various terms as types of advice. The Commissioner's criteria for *advice* are that it should be:

- sought or expected, or be part of the responsibility of a person by virtue of that person's position;
- directed toward taking an action, including making a decision; and
- made to someone who can take or implement the action.

See *IPC Order 96-006* for further explanation of the definition of advice.

The Commissioner has determined that a statement of fact that is not directed toward action to be taken does not qualify as advice under this provision of **section 23** (see *IPC Order 97-007)*.

If the factual information is sufficiently interwoven with other advice that it cannot reasonably be considered separate or distinct, it qualifies under this exception (see *IPC Order 99-001*).

Section 23(1)(a) would not normally apply to the details of a study or background paper where factual information is presented to describe certain issues, problems or events. Rather, it applies to the information used to formulate possible directions in dealing with an issue or problem, to establish a policy or to make a decision.

The nature and significance of many issues are such that disclosure of advice relating to them could reveal information that would cause great damage to the internal processes of decision-making in a public body. Disclosure could also affect its overall ability to effectively manage programs and activities.

It is equally true that there are other issues where more openness surrounding the advisory and decision-making process can be of benefit. There are also issues and activities of lesser significance where the disclosure of advice would have little or no effect on the overall administration or operation of the program or activity.

This section is intended to provide a zone of confidentiality around the policy-making process, rather than protecting all forms of advice (see *IPC Order 99-001*). The public body, within these general parameters, can exercise discretion.

Consultations or Deliberations (section 23(1)(b))

This section allows discretion to refuse access to those records or parts of records containing *consultations or deliberations* involving officers or employees of a public body, a minister or a minister's staff.

A *deliberation* is a discussion or consideration by a group of individuals of the reasons for and against a measure.

A *consultation* is a very similar activity where the views of one or more individuals are sought about the appropriateness of particular proposals or suggested actions.

This discretionary exception is provided for the purpose of permitting the frank exchange of views among a number of individuals whose employment responsibilities include a consultative function.

Within public bodies, consultations and deliberations are normally carried on in an organized manner through the exchange of memoranda and proposals.

Agendas and minutes of meetings are also typical documents that may reveal consultations and deliberations. There is no blanket coverage for such records, but consultative and deliberative material may be severed from records of this nature.

The provision covers consultations or deliberations at all levels in a public body and also those involving a minister or his or her staff.

Positions, Plans, Procedures, Criteria or Instructions Developed for the Purpose of Contractual or Other Negotiations (section 23(1)(c))

This discretionary exception covers the strategies, plans, approaches and bargaining positions that have been employed or are contemplated for the purposes of contractual and other negotiations. It applies to individual public bodies and to the provincial government as a whole. Access to such information can be refused even after particular negotiations have been completed.

Positions and plans refers to information that may be used in the course of negotiations.

Procedures, criteria, instructions and considerations are much broader in scope, covering information relating to the factors involved in developing a particular negotiating position or plan.

Examples of the type of information that could be covered by this exception are the various positions developed by government or local public body negotiators for the purpose of bargaining in relation to labour, financial and commercial contracts.

The exception extends to situations where an agent retained for these purposes carries out negotiations on behalf of the government or a public body.

Plans Relating to the Management of Personnel or Administration of the Public Body (section 23(1)(d))

This provision covers plans relating to the internal management of public bodies, including information about the relocation or reorganization of government departments and agencies, as well as reorganization within local public bodies.

The provision applies only within a limited time frame. Once a plan has been put into operation, the information relating to it can no longer be protected under this exception.

Management of personnel comprises all aspects of the management of human resources of a public body. This includes staffing requirements, job classification, recruitment and selection, employee salary and benefits, hours and conditions of work, leave management, performance review, training, separation and layoff. It also includes the management of personal service contracts.

Administration of a public body comprises all aspects of a public body's internal management, other than personnel management, that are necessary to support the delivery of programs and services. Administration includes business planning, and financial, materiel, contracts, property, information, and risk management.

Although the final plan must be released, the options that were considered before deciding on the plan need not be disclosed. Plans that are never implemented can be protected for 15 years, if there is reason to believe that injury or harm to the efficiency of the operation of the public body could reasonably be expected to result from disclosure.

Implementation means the point when the implementation of a decision begins. For example, a public body decides to go forward with an internal budget cut or restructuring of departments. Implementation commences when this plan of action is communicated to its organizational units.

Contents of Draft Legislation, Regulations and Orders (section 23(1)(e))

This provision covers bills, regulations and orders of members of the Executive Council or the Lieutenant Governor in Council prior to publication, while they are being drafted and formulated in preparation for presentation to the Legislature, publication or public consultation. This provision covers all the drafts and not just the final draft of legislation, regulations and ministerial orders.

For draft by-laws and other legal instruments of local public bodies, see section 4.10 of this chapter.

Contents of Agendas or Minutes of Meetings of the Governing Body of an Agency, Board, Commission, Corporation, Office or Other Body that is a Public Body (section 23(1)(f))

This exception applies only to those public bodies listed in **Schedule 1** of the FOIP Regulation.

The provision establishes agendas and minutes of meetings as classes of record that can be protected because the meetings to which they relate provide the focus for decision-making within these types of bodies. The exception can be applied only to the records of the governing body or a committee of the governing body of the organization.

The exception covers only agendas and minutes of meetings, and not the background reports or studies used in a meeting. Background information must be released unless another exception applies.

Pending Policy and Budgetary Decisions (section 23(1)(g))

This provision covers information, including the proposed plans, policies or projects of a public body, the disclosure of which could reasonably be expected to result in disclosure of a pending policy or budgetary decision. It provides protection from premature disclosure of a policy or budgetary decision.

Once a policy or budgetary decision has been taken and is being implemented, the information can no longer be protected under this provision. A decision is being implemented once those expected to carry out the activity have been authorized and instructed to do so.

Formal Research and Audit Reports that are Incomplete (section 23(1)(h))

This provision covers the contents of formal research and audit reports that, in the opinion of the head of the public body, are incomplete. It provides protection against premature disclosure of information that could be misleading, inaccurate or incomplete.

Formal means that the research or audit reports have been compiled in accordance with procedures that ensure the validity of the research or audit process. The research or audit is carried out in accordance with a prescribed methodology to ensure the greatest degree of accuracy for the results.

Audit is defined as a financial or other formal and systematic examination or review of a program, portion of a program or activity (**section 23(3)**).

Incomplete means that the report is in preliminary or draft format, is under review for accuracy or completeness, or is being reviewed to ensure that it meets the mandate of the research or audit proposal.

For this provision to apply, there should be some evidence that the research or audit report has not been finalized.

For example, if a consultant's research report had been accepted by a public body and payment made in full without any indication that the report had not fulfilled the mandate set out in the contract, the report would be complete. A report submitted by an auditor to officials of a public body for review and discussion prior to its formal presentation would be incomplete.

This exception applies only within a limited time frame. Once the report is accepted as complete, it cannot be protected under this exception. If the report is submitted but no further progress is made on it for a period of 3 years, it cannot be protected under this exception.

Progress implies some activity designed to finalize or complete the report, not simply a review of its contents with no subsequent action.

When the Exception Does Not Apply

Section 23(2) provides some specific cases where the exception in **section 23(1)** does not apply.

***Information has been in existence 15 years or more* (section 23(2)(a)):** This provision means that any information contained within a record which has been in existence for 15 years or more cannot be withheld under the exception.
15 years means the period from a particular month and day to a corresponding month and day 15 years later. Other exceptions may still apply to the information.

***A statement of the reasons for a decision that is made in the exercise of a discretionary power or an adjudicative function* (section 23(2)(b)):** This provision requires the release of formal judgments, including the reasons for reaching those judgments. The provision applies when the decision has already been made and is not merely contemplated.

Reasons mean the motive, cause or justification or facts leading to a decision.

Exercise of discretionary power is normally granted under statute to the administrative level of government. There is discretionary power when, given certain factual circumstances, the administrative authority is free to make a particular decision, given a range of options from which to choose.

Adjudicative function means a function conferred upon an administrative tribunal, board or other non-judicial body or individual that has the power to hear and rule on issues involving the rights of people and organizations.

Examples would be a school board hearing an appeal under the *School Act*, or a hearing by an assessment review board.

Reasons for decisions of this type cannot be withheld under **section 23(1)** despite the fact that the decisions may contain advice or recommendations prepared by or for a minister or a public body.

***Results of product or environmental testing* (section 23(2)(c)):** This provision excludes from the coverage of **section 23(1)** the results of product or environmental testing carried out by or for a public body. The testing has to be complete or have had no progress made on it for at least 3 years.

Examples would be information on a product such as air filters or the results of environmental testing at a land fill or testing of air quality in a building.

It does not apply to testing done:

- for a fee as a service to a person other than a public body; or
- for the purpose of developing methods of testing or testing products for possible purchase.

Examples of test results covered under the exception would be the results of commercial product testing and soil testing. As well, the information may be withheld if the testing was done for the purpose of developing methods of testing. An example might be testing to develop a new drug evaluation methodology. There would have to be evidence in such cases that methodology development was the sole purpose of the testing.

The exception also covers test results where testing was done by a public body in order to determine whether or not to purchase a product.

***Statistical survey* (section 23(2)(d)):** This provision excludes from the coverage of **section 23(1)** statistical surveys.

Statistics is the science of collecting and analyzing numerical data and the systematic presentation of such facts.

Statistical surveys are general views or considerations of subjects using numerical data. Such reports may not be withheld under **section 23(1)**. Where statistical surveys appear with information that can be withheld under **section 23(1)**, the excepted information should be severed and the statistical survey disclosed.

An example of a statistical survey would be a study of growth rates in various forested areas of northern Alberta. Such a study would have to be released even though it may be part of a larger document dealing with reform of forestry law, regulation or policy.

***The result of background research of a scientific or technical nature undertaken in connection with the formulation of a policy proposal* (section 23(2)(e)):** This provision excludes from the coverage of **section 23(1)** background research undertaken as the basis of formulating a policy proposal.

Background research encompasses a wide range of study, review and fieldwork aimed at analyzing and presenting an overview of issues.

For this provision to apply, the research has to be completed or have had no progress made on it for at least 3 years.

The research is to be scientific (conducted according to the principles of objective research) or technical (based on a particular technique or craft) and aimed at policy formulation. In order for information to be considered background research under this provision, it must be connected with the development of some specific policy. This would clearly be the case, if, for example, a policy proposal referred directly to the research on which the proposal was based.

Normally the research methodology, data and analysis cannot be withheld under **section 23(1)**. However, advice and recommendations contained in the same record as the background research or prepared separately by or for a public body or a minister could be withheld.

***An instruction or guideline issued to the officers or employees of a public body* (section 23(2)(f)):** This provision excludes from the coverage of **section 23(1)** information used by officials in interpreting legislation, regulations or policy. It also excludes information used in exercising the discretion given to them under an Act of the Legislature or a by-law of a local public body.

Generally, an official or employee in a position to provide interpretation or policy direction will have issued the instruction or guideline.

***A substantive rule or statement of policy that has been adopted by a public body for the purpose of interpreting an Act or regulation or administering a program or activity of the public body* (section 23(2)(g)):** This provision expands on the principles set out in **section 23(2)(f)**. It excludes from the coverage of **section 23(1)** the basic interpretations of the law, regulations and policy under which a public body operates its programs and activities.

This provision complements **section 84(1)** of the *Act*, which requires that public bodies have in place facilities where the public may examine any manual, handbook or other guideline used in decision-making processes that affect the public.

Application of Exception

Figure 9 contains a flowchart setting out the steps for applying **section 23**.

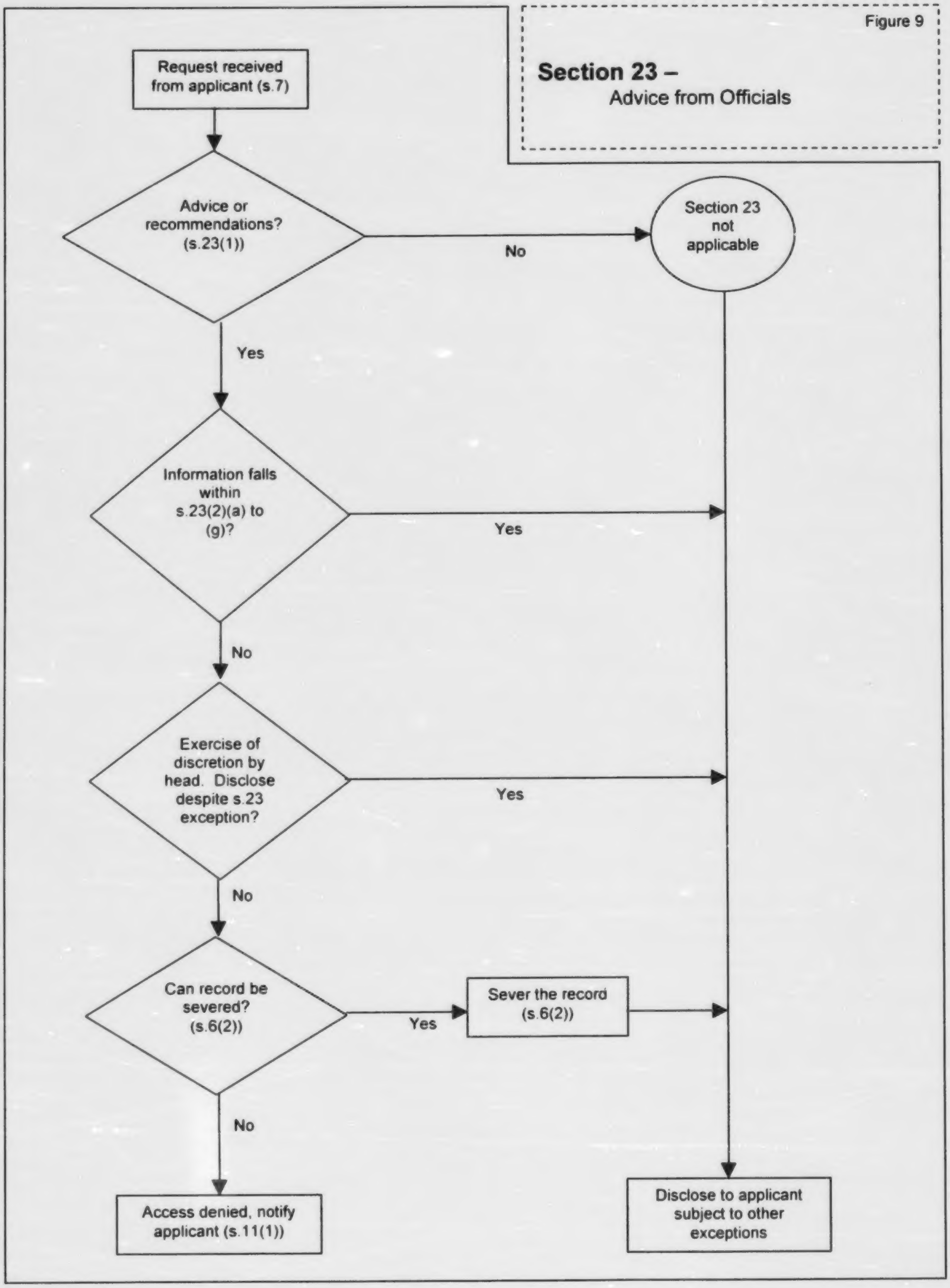


Figure 9

Section 23 –
Advice from Officials

Request received from applicant (s.7)
Advice or recommendations? (s.23(1))
No
Section 23 not applicable
Yes
Information falls within s.23(2)(a) to (g)?
Yes
No
Exercise of discretion by head. Disclose despite s.23 exception?
Yes
No
Can record be severed? (s.6(2))
Yes
Sever the record (s.6(2))
No
Access denied, notify applicant (s.11(1))
Disclose to applicant subject to other exceptions

4.12 ECONOMIC AND OTHER INTERESTS OF A PUBLIC BODY OR THE GOVERNMENT OF ALBERTA

Overview

Section 24(1) of the *Act* provides that a public body may refuse to disclose information if the disclosure could reasonably be expected to harm the economic interest of a public body or the Government of Alberta as a whole, or the ability of the government to manage the economy.

Section 24 is a discretionary exception. The information that can be excepted includes:

- trade secrets of a public body or the Government of Alberta (**section 24(1)(a)**);
- financial, commercial, scientific, technical or other information in which a public body or the Government of Alberta has a proprietary interest or a right of use and that has, or is reasonably likely to have, monetary value (**section 24(1)(b)**);
- information the disclosure of which could reasonably be expected to:
  - result in financial loss to,
  - prejudice the competitive position of, or
  - interfere with contractual or other negotiations of

  the Government of Alberta or a public body (**section 24(1)(c)**); and
- information obtained through research by an employee of a public body, the disclosure of which could reasonably be expected to deprive the employee or the public body of priority of publication (**section 24(1)(d)**).

This exception allows the public body discretion to protect information if its disclosure could harm either its own financial or economic interests or those of the Government of Alberta as an entity. It also protects information that would harm the ability of the Government of Alberta to manage the economy.

The exception refers to the *Government of Alberta* as a whole. This recognizes that public bodies, individually or collectively, may hold significant amounts of financial and economic information that is critical to the financial management of the public sector and the management of the provincial economy. **Section 24(1)** ensures that, where harm would result from disclosure, certain portions of this information may be withheld.

Harms Test

In order to use the exception, a public body must have objective grounds to believe that disclosure will likely result in the harm. The context in which a public body operates is taken into account in determining whether it is reasonable to expect that harm will result from the disclosure of the information.

Economic interests refers to both the broad interests of a public body and, for provincial public bodies, of the government as a whole, in managing the production, distribution and consumption of goods and services.

It also covers financial matters such as the management of assets and liabilities by a public body and the public body's ability to protect its own or the government's interests in financial transactions.

The *financial interests* of the Government of Alberta include the ability to collect taxes and generate revenues.

Harm to these interests includes damage or detriment to the economic policies or activities for which a single public body is responsible, as well as harm to policies and programs that affect the overall economy of the province. It also includes monetary loss or loss of assets with monetary value.

Examples of information the disclosure of which might qualify for harm to economic interests include:

- information on a public body's investment strategies which affects its interests or future financial position;
- information in budget preparation documents that could result in segments of the private sector taking actions affecting the ability of the government or a local public body to meet economic goals;
- information about licensing and inspection practices of a public body that could affect the amount of revenue collected; and
- information about a trade deal, a development plan or strategy or an economic negotiation that has not been completed.

Section 24(1) does not prevent the release of information that reveals a liability that might lead to a lawsuit against a public body for alleged wrongdoing.

In most cases, the public body whose economic interests are involved will be the public body with custody or control of the record(s) requested.

In some instances, however, a public body may hold information about another public body whose economic interests may be affected by disclosure. Consultation is essential between the two bodies in situations when use of **section 24(1)** is being considered.

Interests of the Government of Alberta

The exception may also be claimed for the *Government of Alberta* in the broad, corporate sense. The term *Government of Alberta* connotes a broader sense here than that of public body. The exception has a different and higher level coverage, since *government* is intended to convey the sovereign power of the state in carrying out its will and functions.

The phrase *ability to manage the economy* refers to the responsibility of the Government of Alberta to manage the province's economic activities by ensuring that an appropriate economic infrastructure is in place, and by facilitating and regulating the activities of the marketplace.

This depends on a range of activities including fiscal and economic policies, taxation, and economic and business development initiatives.

Types of Information

The types of information listed in **section 24(1)** are illustrative only and may not cover all types of information that could reasonably be expected to cause harm to economic interests. At the same time, inclusion in one of the categories in **section 24(1)** is not by itself sufficient to allow a public body to refuse access. Application of this exception is subject to a harms test.

A public body must have reasonable grounds to expect harm as a result of disclosure in order to apply the exception.

***Trade secret* (section 24(1)(a)):** *Trade secret* is defined in **section 1(1)(s)** of the *Act* as meaning information, including a formula, pattern, compilation, program, device, product, method, technique or process:

- that is used, or may be used, in business or for any commercial purpose;
- that derives independent economic value, actual or potential, from not being generally known to anyone who can obtain economic value from its disclosure or use;
- that is the subject of reasonable efforts to prevent it from becoming generally known; and
- the disclosure of which would result in significant harm or undue financial loss or gain.

Information must meet *all* of these criteria to be considered a trade secret.

Information that is generally available through public sources (e.g., published research reports) would not usually qualify as a trade secret under the *Act*.

A public body must own trade secrets or must be able to prove a claim of legal right in the information (e.g., a licence agreement) in order to qualify for the exception. Normally, this will mean that the trade-secret information has been created by employees of the public body as part of their jobs, or by a contractor as part of a contract with the public body.

For example, software developed by a public body or special testing equipment, which is not generally known, would have commercial value. Disclosure of the specifications could reasonably be expected to result in improper benefit and the information could probably qualify as a trade secret. On the other hand, details of a minor technical adjustment to equipment that has been inspired by an article in a trade journal would not qualify.

Section 24(1)(a) does not apply to trade secrets of a third party. Requirements relating to the protection of these are dealt with in **section 15(1)(a)**. See section 4.3 of this chapter.

***Financial, commercial, scientific, technical or other information in which a public body or the Government of Alberta has a proprietary interest or a right of use and that has, or is reasonably likely to have, monetary value* (section 24(1)(b)):** The exception in this provision is subject to a three-part test. In order for the exception to apply, *all* of the following conditions must be met:

- the information must be financial, commercial, scientific, technical or other information;
- the public body or the Government of Alberta must have a proprietary interest or a right of use; and
- the information must have, or be reasonably likely to have, monetary value.

Financial information refers to information relating to money and its use or distribution, or assets with monetary value, such as securities or stock options. Common examples are investment strategies and financial forecasts.

Commercial information refers to information concerning the sale, purchase or exchange of goods and services. Examples include marketing plans, pricing structures and customer records.

Technical information means information relating to a particular subject, craft or technique, such as systems design specifications.

Scientific information relates to experiments, principles and procedures derived by scientific method.
An example would be a particular scientific testing methodology.

The second part of the test requires that the public body or the Government of Alberta have a *proprietary interest* in the information. This means that the public body or the government must be able to demonstrate rights to the information. For example, a municipality may have a proprietary interest in geographical information systems mapping data or statistical data.

The third part of the test is whether the information has or is reasonably likely to have monetary value. *Monetary value* may be demonstrated by potential for financial return to the public body or government. An example of information that is reasonably likely to have monetary value might include a course developed by a teacher employed by a school board.

Information the disclosure of which could reasonably be expected to result in financial loss to, prejudice the competitive position of, or interfere with contractual or other negotiations of the Government of Alberta or a public body **(section 24(1)(c):**
This section provides similar protection for business enterprises in the public sector as is provided for private sector third parties under **section 15(1)(c)**.
To claim the exception, a public body must have objective grounds for believing that one of the harms listed will result from disclosure.

In the case of *financial loss*, there must be reasonable grounds to believe that disclosure of information in the specific record would result in direct monetary loss or loss in terms of a monetary equivalent. This includes loss of revenue, loss of reputation or loss of good will in the marketplace. The loss cannot be speculative nor can it be loss expected as a result of a "ripple effect" (see *IPC Order 98-020*).

Prejudice to competitive position means that a public body must have a reasonable expectation that disclosure of the information is capable of being used by an existing or potential competitor to reduce the public body's or the government's share of a market. However, the exception may be claimed whether or not there is currently a competitor in the marketplace.

Interfere with contractual or other negotiations means obstruct or make much more difficult the negotiation of a contract or other sort of agreement between the public body or the government and a third party. The expectation of interference with negotiations as a result of disclosure must be reasonable and the negotiations have to be specific, not simply potential negotiations of a general kind in the future (see *IPC Order 98-005*).

***Information obtained through research by an employee of a public body, the disclosure of which could reasonably be expected to deprive the employee or public body of priority of publication* (section 24(1)(d)):** Public bodies employ a wide range of researchers, including professional scientists, technicians and social scientists. Their reputations are often dependent on the research they publish.

The fact that they have a professional reputation is of considerable value to public bodies that employ them. In addition, their research often has monetary and program value for the public bodies. For these reasons, the *Act* protects the priority of publication for all types of research.

Examples include scientific and technical research carried out at research institutes or universities; historical research connected with the designation or preservation of historical or archeological resources; and epidemiological and other medical studies carried out in health care bodies. A public body would have to provide some proof that publication is expected to result from the research or that similar research in the past has resulted in publication.

When the Exception Does Not Apply

Section 24(2) provides that a public body must not refuse to disclose under **section 24(1)** the results of product or environmental testing carried out by or for a public body, unless the testing was done:

- for a fee as a service to a person, other than the public body (**section 24(2)(a)**); or
- for the purpose of developing methods of testing or testing products for possible purchase (**section 24(2)(b)**).

The intent of the provision is to ensure that a public body does not withhold information resulting from product or environmental testing carried out either by the employees of a public body or on its behalf by another organization.

Examples include information on products such as air filters and environmental test results on water quality or air quality.

Information can be withheld when the public body performs the testing, for a fee, as a service to a private citizen or private corporate body.

Common examples are commercial product testing and soil testing.

The information may also be withheld if the testing was done for the purpose of developing methods of testing. An example might be testing to develop a new drug evaluation methodology. There would have to be evidence in such cases that methodology development was the sole purpose of the testing.

The exception can also be used to withhold test results compiled to determine whether or not a public body would purchase a product.

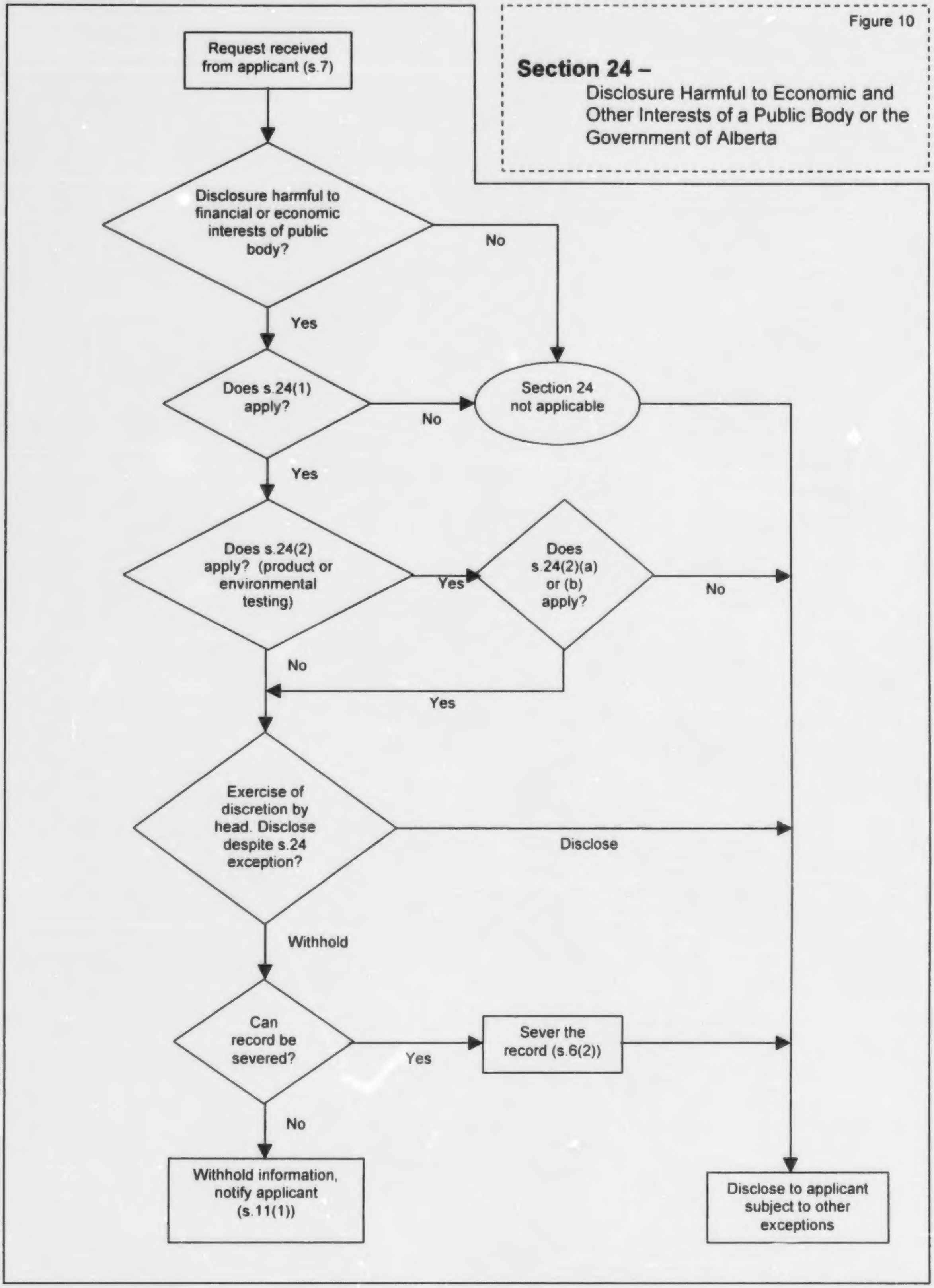
In all three circumstances, the harms test in **section 24(1)** still has to be met before the information can be withheld.

Applying the Exception

Figure 10 contains a flowchart setting out the steps for applying **section 24**.

Figure 10

Section 24 –
Disclosure Harmful to Economic and Other Interests of a Public Body or the Government of Alberta


Request received from applicant (s.7)
Disclosure harmful to financial or economic interests of public body?
No
Yes
Does s.24(1) apply?
No
Section 24 not applicable
Yes
Does s.24(2) apply? (product or environmental testing)
Yes
Does s.24(2)(a) or (b) apply?
No
No
Yes
Exercise of discretion by head. Disclose despite s.24 exception?
Disclose
Withhold
Can record be severed?
Yes
Sever the record (s.6(2))
No
Withhold information, notify applicant (s.11(1))
Disclose to applicant subject to other exceptions

4.13 TESTING PROCEDURES

Section 25 of the *Act* provides that a public body may refuse to disclose information relating to:

- testing or auditing procedures or techniques (**section 25(a)**);
- details of specific tests to be given or audits to be conducted (**section 25(b)**); or
- standardized tests including intelligence tests (**section 25(c)**).

The exception applies only if the disclosure could reasonably be expected to prejudice the use or results of particular tests or audits.

Section 25 is a discretionary exception.

This exception provides protection for the procedures and techniques involved in testing and auditing. It also protects details relating to specific tests to be given or audits to be conducted.

The terms *test* and *audit* are intended to be interpreted broadly to cover a wide variety of activities undertaken by public bodies or by the private sector on behalf of public bodies. Examples include environmental testing, staffing examinations, personnel audits, financial audits, and program audits.

Specific mention is made of standardized tests such as intelligence tests, psychological tests and aptitude tests, which are often used in educational bodies and health care bodies.

Information is protected where disclosure of a test or audit that is to be conducted, or is currently in process, would invalidate the results. This applies even if there is no intention to use the test or audit again in the future.

Information is also protected where there is an intention to use the procedure in the future, and disclosure would result in unreliable results being obtained and the test or audit having to be abandoned as a result. Test questions that are regularly used – for example, in making staffing – may be protected from disclosure.

Information relating to a test or an audit that has been used in the past, but which is neither in process nor to be used in the future, is not protected by this exception.

The exception applies to testing and auditing carried out both by public bodies and by consultants and contractors.

This section does not provide an exception for the results of tests or audits. This includes the results of standardized tests or intelligence tests. Public bodies should exercise care in disclosing such results by ensuring that a professional familiar with the tests is available to explain and interpret them to the applicant. This process may be specified in policy.

4.14 PRIVILEGED INFORMATION

Overview

Section 26 deals with legal privilege.

Section 26(1) allows the head of the public body discretion to refuse to disclose information subject to legal privilege, with the exception that only the Speaker of the Assembly has the right to determine whether a record is subject to parliamentary privilege.

Section 26(2) is a *mandatory* exception requiring the public body to refuse to disclose privileged information of a third party.

When dealing with information that may qualify for the exception under section 26, public bodies should always consult their legal counsel.

Section 26(1) of the *Act* provides that a public body may refuse to disclose information:

- that is subject to *any type* of legal privilege, including solicitor–client privilege or parliamentary privilege (**section 26(1)(a)**);
- prepared by or for the Minister of Justice and Attorney General, or an agent or lawyer of the Minister of Justice and Attorney General or a public body, in relation to a matter involving the provision of legal services (**section 26(1)(b)**); or
- in correspondence between the Minister of Justice and Attorney General, or an agent or lawyer of the Minister of Justice and Attorney General or a public body, and any other person in relation to a matter involving the provision of advice or other services by the Minister, an agent or lawyer (**section 26(1)(c)**).

Section 26(2) states that a public body *must refuse* to disclose information described in **section 26(1)(a)** if it relates to a person other than the public body.

Section 26(3) makes it clear that only the Speaker of the Legislative Assembly may rule on the question of what is and what is not parliamentary privilege. **Section 62(4)(b)** provides that the Commissioner cannot review the Speaker's ruling (see *IPC Order 97-017)*.

The intent of this section is to ensure that information privileged at law, as well as other similar information in the custody or under the control of a public body, is protected from disclosure in much the same way as an individual's information would be by his or her lawyer.

Section 26 is also intended to protect disclosure of privileged information in the custody or control of a public body that belongs to a third party, as well as information covered by parliamentary privilege.

The *Act* does not define *legal privilege*, so its definition is derived from the common law (see *IPC Order 96-020*).

When information falls within the scope of **section 26(1)**, a public body may decide to disclose the information if the law would otherwise permit disclosure. An example would be when the "owner" of the privilege consents to disclosure (see *IPC Order 97-003*).

Under **section 26(2)**, if there is information subject to any type of legal privilege, including solicitor–client privilege or parliamentary privilege, that relates to (i.e., belongs to) a person other than a public body, a public body *must not disclose* that information. It does not have any discretion (see *IPC Order 96-020*).

Legal Privilege

***Nature of the privilege*:**
Section 26(1)(a) deals with any type of *legal privilege*, noting especially solicitor–client privilege and parliamentary privilege. The Commissioner has found that **section 26(1)(a)** of the *Act* incorporates the common law public interest privilege (see *IPC Order 96-020*).

Public interest privilege refers to a determination of whether information should or should not be disclosed. That determination requires that a decision-maker balance two competing public interests: the public interest in maintaining the confidentiality of certain information and the public interest in disclosing the information.

It consists of two subcategories: "class privilege" and "case-by-case privilege." In the case of the former, which includes solicitor–client privilege and police informer privilege, the balance of two competing interests has been decided in favour of the public interest in maintaining the confidentiality of the information. That means there are overriding policy reasons for maintaining confidentiality.

In the latter case, a public body has to weigh the policy reasons for maintaining confidentiality in each case and determine whether the public interest favours disclosure or non-disclosure (see *IPC Order 96-020*).

Class Privileges

***Solicitor–client privilege*:** A common example of a class privilege is solicitor–client privilege.
If a record is subject to solicitor-client privilege, it means that the record is confidential and does not have to be disclosed (see *IPC Order 96-017*).

There are two kinds of solicitor–client privilege. **Section 26(1)(a)** encompasses both of them:

- solicitor and client communications; and
- third party communications prepared in anticipation of litigation and subject to what is often referred to as *litigation privilege* (see *IPC Order 96-017*).

The point of solicitor–client privilege is to protect legal advice, and not solely the confidential aspect of the professional relationship. Otherwise, it would not be necessary to examine each record to determine whether solicitor–client privilege applies (see *IPC Order 96-015*).

The presence of an agent does not destroy solicitor–client privilege, as long as the communication through the agent meets the tests set out below (see *IPC Order 97-003*).

***Severing* is *not* a concept applicable to records subject to solicitor–client privilege. Therefore, the privilege must be claimed for the entire record or not at all** (see *IPC Order 96-017*).

Severing is not a concept recognized at common law.

Solicitor–client communications: In the case of solicitor–client communications, each record must meet the following criteria for the privilege to apply:

- it is a communication between solicitor and client;
- it entails the seeking or giving of legal advice; and
- it is intended to be confidential by the parties (see *IPC Order 96-017* and *IPC Order 96-021*).

The information must be contained in a communication between a solicitor and a client. A memorandum or note from one employee of a public body to another summarizing a conversation between that employee and the public body's lawyer does not meet this criterion. It may, however, meet the criterion of **section 26(1)(c)**, information in correspondence between a public body and any other person in relation to a matter involving the provision of advice by the lawyer as noted below (see *IPC Order 96-019*).

The term *legal advice* is defined to include a legal opinion about a legal issue, and a recommended course of action, based on legal considerations, regarding a matter with legal implications (see *IPC Order 96-017*).

Both parties must intend the communication to be confidential, and must demonstrate that this confidentiality has been maintained. If confidentiality is not maintained, privilege is waived and this provision does not apply (see Waiver of Privilege below).

A client's communication with his or her solicitor solely to convey or receive factual information may not be privileged under these criteria because the communication does not entail the seeking or giving of legal advice. An example might be an invoice or the cover sheet of a facsimile transmission. On this premise, a solicitor's request to the client for factual information would also not be privileged (see *IPC Order 96-015*).

The Information and Privacy Commissioner has the jurisdiction to apply these criteria to a record to determine whether solicitor–client privilege exists. However, the Commissioner has stated that he has no jurisdiction to delve into any record to determine what part of a solicitor–client communication is factual and therefore not privileged under the rules relating to discovery of documents in court cases.

In other words, only the courts can determine what parts of a document are factual and can be disclosed. The Commissioner has stated that if solicitor–client privilege applies, it applies to the entire document. He has no jurisdiction either to determine the factual component under the Rules of Court, or to require that the public body sever that document under the *Act* (see *IPC Order 98-004*).

The following substantive rules will also be considered when a claim for solicitor–client privilege is made:

- the confidentiality of communications between solicitor and client may be raised in any circumstances where such communications are likely to be disclosed without the client's consent;

- unless the law provides otherwise, when and to the extent that the legitimate exercise of a right would interfere with another person's right to have his or her communications with his or her lawyer kept confidential, the resulting conflict should be resolved in favour of protecting the confidentiality;
- when the law gives someone the authority to do something which, in the circumstances of the case, might interfere with that confidentiality, the decision to do so and the choice of means of exercising that authority should be determined with a view to not interfering with it except to the extent absolutely necessary in order to achieve the ends sought by the enabling legislation; and
- legislation referred to above must be interpreted restrictively

(See *IPC Order 96-017.*)

Records such as solicitor's briefing notes and working papers directly relating to the seeking or giving of legal advice may be excepted under this branch of solicitor–client privilege (see *IPC Order 96-017*).

Where a communication between a solicitor and client constitutes a continuum of advice, such communication is privileged (see *IPC Order 96-020* and *IPC Order 96-021*).

Litigation privilege: The criteria for litigation privilege are different from those that apply to solicitor–client communications. To correctly apply this branch of solicitor–client privilege, the public body must show that:

- there is a third party communication which may include:
  - communications between the client (or the client's agents) and third parties for the purpose of obtaining information to be given to the client's solicitors to obtain legal advice,
  - communications between the solicitor (or the solicitor's agents) and third parties to assist with the giving of legal advice, or
  - communications which are created by the client, including reports, schedules, briefs, documentation, etc.;
- the maker of the record or the person under whose authority the record was made intended the record to be confidential. The one exception is for the lawyer's "work product" or "lawyer's brief" for which it is the lawyer's intention that is relevant when the lawyer assembles material for the brief for litigation;
- the *dominant purpose* for which the records were prepared was to submit them to a legal advisor for advice and use in litigation, whether existing or contemplated. The *dominant purpose* test consists of three requirements:
  - the records must have been *produced* with existing or contemplated litigation in mind;
  - the records must have been produced for the *dominant purpose* of existing or contemplated litigation; and
  - if litigation is contemplated, the prospect of litigation must be *reasonable* (see *IPC Order 97-009* and *IPC Order 96-015*);

and

- there must be proof that the third party records were actually sent to the public body's solicitors (see *IPC Order 98-004*).

The guiding principle for litigation privilege is that all papers and materials created or obtained especially for the lawyer's brief for litigation, whether existing or contemplated, are privileged. This means that such papers and materials are confidential and do not have to be disclosed.

The privilege applies to papers and materials:

- created or obtained by the client for the lawyer's use in existing or contemplated litigation; or
- created by a third party or obtained from a third party on behalf of the client for the lawyer's use in existing or contemplated litigation

(See *IPC Order 96-015.*)

When determining *dominant purpose*, the intent of the maker of the record or the person under whose authority the record was made is to be considered. Furthermore, the maker of the record or the person under whose authority the record was made *must* have intended the record to be confidential, with the possible exception of the "work product" or "lawyer's brief" rule (see *IPC Order 96-015*).

Waiver of the privilege: The right to solicitor–client privilege belongs to the client and not the lawyer, and may be waived by the client. This allows a public body to disclose records that fall within the parameters of **section 26(1)**.

Waiver can occur in one of two ways:

- an intention to waive the privilege; or
- more commonly, a waiver by implication.

An example of where an intention to waive occurs is when the client specifically waives the privilege. This may occur through a decision to disclose information to a third party, whether in response to an access request under the *FOIP Act* or not, or through widespread dissemination of the information.

This does not occur when records are copied to lawyers or employees within the public body (see *IPC Order 96-017* and *IPC Order 96-021*).

Nor does it occur when records have been copied to legal firms which provided solicitors to represent the public body, or to the Minister to whom the public body reports (see *IPC Order 96-020*).

Privilege is not waived when an individual is obliged to comply with a public body's requirements under penalty of enforcement proceedings for non-compliance (see *IPC Order 98-017*).

Waiver by implication is less clear. Waiver in these circumstances may occur where fairness and consistency require it, such as in a court case where the client directly makes an issue out of the legal advice given. There can also be a *deemed waiver* where part of a record containing solicitor–client privilege is released or where privilege is not claimed for the entire communication on a page (see *IPC Order 96-017*).

If a public body cannot provide evidence that the person who received a communication intended to maintain confidentiality, the public body can be found to have waived solicitor–client privilege (see *IPC Order 96-017* and *IPC Order 96-019*).

There can be a *limited waiver* of privilege, which does not extend to a waiver for other purposes. For example, a third party might voluntarily provide public documents to a public body, but that does not constitute a waiver of privilege to other parties. There can also be a privilege in aid of anticipated litigation in which several persons have a common interest such that, in providing records to each other, the parties with common interests do not waive privilege as against other parties or the world at large. In considering whether a limited waiver can stand, it will be important to check to whom records may have been formally copied (see *IPC Order 96-009*).

Police informer privilege: Another class privilege is an informer, historically known as *police informer privilege*.

This privilege prevents not only disclosure of the name of the informer, but also any information that might implicitly reveal identity, even if it is the smallest detail (see *IPC Order 96-020*).

The privilege afforded to police informers has been granted in order to give protection to citizens who assist in law enforcement. These individuals may very well be vulnerable to reprisals from those against whom they inform.

The policy reason behind the privilege is to protect this source of information since, without the privilege, the information would likely not be provided. The end result would be that the policing agencies would be impaired in their efforts to detect and prevent crime (see *IPC Order 96-021*).

Although the privilege belongs to the Crown, the privilege also belongs to the informer. The only way the privilege can be waived is with the informer's consent, or, in the case of an anonymous informer, by the Crown.

The privilege is subject to only one exception: "innocence at stake." To raise this exception, there must be a basis on the evidence for concluding that disclosure of the informer's identity is necessary to demonstrate the innocence of someone in a criminal proceeding (see *IPC Order 96-020*).

An analogy may be made to police informer privilege in other situations. It will be necessary to show that the public interest in protecting communications to government agencies by informers outweighs the public interest in requiring that the information be produced in proceedings under the relevant legislation such as the *FOIP Act*.

This occurs when the public body requires this information in order to administer legislation dealing with public health and safety (see *IPC Order 96-020* and *IPC Order 96-021*).

Examples might include a complaint to the Alberta Health Facilities Review Committee about patient treatment in a hospital, or a report of abuse made under the *Protection for Persons in Care Act*. Evidence of confidentiality will be required.

This does not apply to employees of a public body whose job it is to provide information about suspected fraud or other infringements of legislation that they administer (see *IPC Order 99-010*).

Parliamentary privilege:
Parliamentary privilege is a unique class privilege that provides the necessary immunity to allow members of the Legislative Assembly to do their legislative work.

Section 26(3) provides a mechanism for determining when information may be subject to parliamentary privilege. This is done through the Speaker of the Legislative Assembly.

If the Speaker makes a ruling that records are subject to parliamentary privilege, the Information and Privacy Commissioner has no jurisdiction to review a decision of a public body to refuse to provide access to those records (**section 62(4)(b)** of the *Act*).

In addition, the Speaker remains free to make such a determination even after the Information and Privacy Commissioner has decided that the records are not subject to exceptions contained in the *Act* (see *IPC Order 97-017*).

When a public body believes that all or parts of the records that are the subject of a request may be subject to parliamentary privilege, it must provide notice to the Speaker of the Legislative Assembly. The notice must include a description of the contents of the record(s) and a request that the Speaker determine whether or not parliamentary privilege does apply to some or all of the information. The decision of the Speaker *must* be followed.

Model Letter J in Appendix 3 of this publication may be used to request a determination from the Speaker.

***Legislated privilege*:** A class legal privilege also can be established by an Act or by a regulation (see *IPC Order 96-020*).

For example, section 24(3) of the *Ombudsman Act* states that anything said or any information supplied or any record, paper or thing produced by any person in the course of any inquiry by or proceedings before the Ombudsman is privileged in the same manner as if the inquiry or proceedings were proceedings in a court.

***New class of privilege*:** It has been said that to find a new class of privilege for private records, compelling policy reasons must exist similar to those underlying the privilege for solicitor–client communications, and the relationship must be inextricably linked with the justice system. Identification of a new class of privilege on a principled basis is not precluded. But it has also been said that the extension of the doctrine of privilege consequently obstructs the truth-finding process and, accordingly, the law has been reluctant to proliferate areas of privilege unless an external social policy is demonstrated to be of such unequivocal importance that it demands protection (see *IPC Order 96-020*).

Case-By-Case Privileges

For a case-by-case privilege to exist, the decision-maker must determine whether the public interest favours disclosure or non-disclosure in a particular case (see *IPC Order 96-020*).

Records may be either *private records* or *Crown records*. *Crown records*, that is, provincial government records, include records containing information relating to activities, operations or decisions at the highest level of the provincial government such as Cabinet decisions (see *IPC Order 96-020*). The concept of Crown records relates only to provincial government bodies.

Private records: Private records are records in the hands of a third party where there is a reasonable expectation of privacy, such as medical or therapeutic records, school records, private diaries, and social worker activity logs, etc. For a case-by-case privilege to apply to private records, the following criteria must be met:

- the communications must originate in a confidence that they will not be disclosed;
- this element of confidentiality must be essential to the full and satisfactory maintenance of the relationship between the parties;
- the relationship must be one which in the opinion of the community ought to be diligently fostered; and
- the injury that would result to the relation by the disclosure of the communications must be greater than the benefit gained for the correct disposal of the litigation.

The criterion that the injury from disclosure must be greater than the benefit from disclosure for the privilege to apply requires an assessment of the interests served by protecting communications from disclosure. This includes privacy interests and the inequalities that may be perpetuated by the absence of protection. The balancing exercise under this criterion is essentially one of common sense and good judgment. It must also be kept in mind that a request for access and an inquiry under the *Act* are not litigation.

The balance to be struck is that the injury to the relationship from the disclosure of the information must be greater than an applicant's right of access to the information under the *Act*. An informer's privacy interests are struck at a different level in a proceeding under the *Act* than in civil proceedings and more easily outweigh an applicant's right of access under the *Act* (see *IPC Order 96-020* and *IPC Order 96-021*).

Crown records: Public interest immunity or Crown privilege: Historically, the privilege for Crown records has been called *Crown privilege*. It is more properly called *public interest immunity* because there must be a balancing of two competing public interests:

- the public interest in non-disclosure to maintain government secrecy; and
- the public interest in disclosure for the proper administration of justice (see *IPC Order 96-020*).

For a case-by-case privilege to attach to Crown records, the Crown must put forward a claim based on the following criteria for public immunity:

- the nature of the policy concerned;
- the particular contents of the records;
- the level of the decision-making process;
- the time when a record or information is to be revealed;
- the importance of producing the records in the administration of justice, with particular consideration to
  - the importance of the case,
  - the need or desirability of producing the records to ensure that the case can be adequately and fairly represented; and
  - the ability to ensure that only the particular facts relating to the case are revealed; and
- any allegation of improper conduct by the executive branch towards a citizen (see *IPC Order 96-020*).

Privilege Relationship with Legal Agent

Section 26(1)(b) and **(c)** deal with circumstances where a legal privilege may not exist.

Section 26(1)(b) is about information prepared by or for an agent or lawyer of the Minister of Justice and Attorney General or a public body, or by or for the Minister. That information must be prepared *in relation to* a matter involving the provision of legal services.

The term *legal services* is given its ordinary dictionary meaning, and includes any law-related service performed by a person licensed to practice law, including the Minister of Justice and Attorney General.

This provision is broader than solicitor–client privilege (see *IPC Order 96-017*). It appears to protect information that would not be protected by solicitor–client privilege (see *IPC Order 96-015*).

Section 26(1)(c) covers correspondence between an agent or lawyer of the Minister of Justice and Attorney General or a public body, or the Minister, and any other person in relation to a matter involving the provision of advice or other services.

This provision covers only correspondence, and that correspondence must relate to a matter involving the provision of advice or other services by the Minister or the agent or lawyer.

A memorandum or note from one employee of a public body to another summarizing a conversation between that employee and the public body's lawyer may meet this criterion (see *IPC Order 96-019*).

Legal Privilege of Other Persons

Section 26(2) requires public bodies to protect information described in **section 26(1)** when it relates to a person other than a public body.

At times, privileged legal records of an individual or other third party come under the custody or control of a public body. In these circumstances, the public body has an obligation to protect these legal records.

The distinction between this provision and **section 26(1)(a)** is that **section 26(2)** is *mandatory*. The public body must not disclose the information if the criteria in **section 26(1)(a)** and **26(2)** are met (see

IPC Order 96-019 and *IPC Order 96-021*).

This provision speaks of *information* that relates to a person other than the public body and not a *record* or *document*. It is meant to encompass not only another person's records or documents to which the privilege under **section 26(1)(a)** might apply, but also *information*, in any form, to which a privilege applies (see *IPC Order 97-009*).

Records in which a public body has discussed or otherwise reproduced a third party's privileged information may also be covered by this provision (see *IPC Order 97-009*).

Information under **section 26(1)(a)** also "relates to" persons other than a public body if they supplied the information and the information can identify them (see *IPC Order 96-021*).

Even if a record of this nature was disclosed before the coming into force of the *Act*, because **section 26(2)** is a *mandatory* exception, a public body is obliged to apply it if a record is within the scope of the exception (see *IPC Order 97-009*).

The Information and Privacy Commissioner will normally consider whether **section 26(2)** applies to records of a third party that may be subject to legal privilege, even if a public body does not apply the exception (see *IPC Order 96-019*).

Relationship with Section 16, Section 19 and Section 21

Section 16(4)(b) and **section 19(1)(d)** have not incorporated into the *Act* a public interest privilege for private records in the custody or control of the Crown. The *Act* also does not preclude **section 26(1)(a)** from incorporating the common law public interest privilege for private records (see *IPC Order 96-020*).

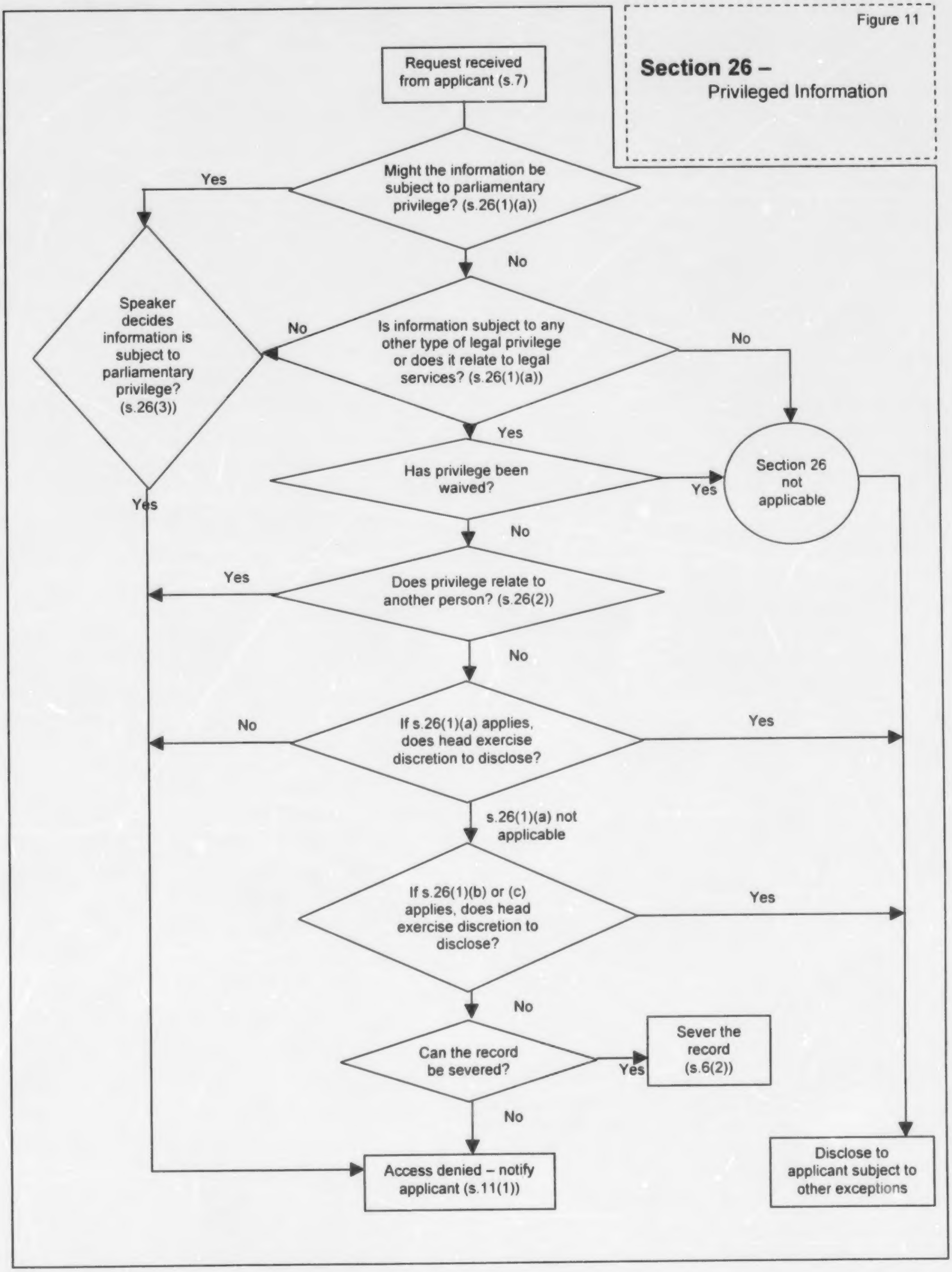
Section 21 of the *Act* does not appear to incorporate the common law as to public interest privilege or public interest immunity for certain specific Crown records, namely Cabinet confidences (see *IPC Order 96-020* and *IPC Order 97-010*).

Applying the Exception

Figure 11 contains a flowchart setting out the steps for applying **section 26**.

Figure 11

Section 26 –
Privileged Information


Request received from applicant (s.7)
Might the information be subject to parliamentary privilege? (s.26(1)(a))
Yes
No
Speaker decides information is subject to parliamentary privilege? (s.26(3))
No
Is information subject to any other type of legal privilege or does it relate to legal services? (s.26(1)(a))
No
Yes
Section 26 not applicable
Has privilege been waived?
Yes
Yes
No
Does privilege relate to another person? (s.26(2))
Yes
No
If s.26(1)(a) applies, does head exercise discretion to disclose?
No
Yes
s.26(1)(a) not applicable
If s.26(1)(b) or (c) applies, does head exercise discretion to disclose?
Yes
No
Can the record be severed?
Yes
Sever the record (s.6(2))
No
Access denied – notify applicant (s.11(1))
Disclose to applicant subject to other exceptions

4.15 DISCLOSURE HARMFUL TO HISTORIC RESOURCES, RARE, ENDANGERED OR VULNERABLE LIFE

Overview

Section 27 provides that a public body may refuse to disclose information if the disclosure could reasonably be expected to result in damage to or interfere with the conservation of:

- any historic resource as defined in the *Historical Resources Act* (section 1(f)) **(section 27(a))**; or
- any rare, endangered, threatened or vulnerable form of life (**section 27(b)**).

Section 27 is a discretionary exception.

It enables a public body to protect information about historic resources, which, if disclosed, could result in damage to these resources or interference with conservation measures. If a public body has records that might fall under this exception, it may consult with the ministry responsible for the *Historical Resources Act* in making a decision on disclosure.

In using this exception there must be objective grounds to believe that disclosure is likely to result in damage to historic resources or interference with conservation measures.

Definitions

The *Historical Resources Act* defines *historic resources* as any work of nature or of man that is primarily of value for its palaeontological, archaeological, prehistoric, historic, cultural, natural, scientific or aesthetic interest, including, but not limited to, a palaeontological, archaeological, prehistoric, historic, or natural site, structure or object.

Examples include designated municipal historic resources, designated registered historic resources in private ownership, museum collections, and archaeological and palaeontological sites revealed during a historic resources impact assessment.

Damage refers to destruction, disturbance, alteration, deterioration or reduction in the value of an historic resource.

In **section 27(b)**, the following general definitions apply:

A *rare form of life* is any species of flora or fauna that is in a special category because it does not occur in great abundance in nature, either because it is not prolific or its population or range has been adversely affected by modern civilization.

An *endangered form of life* is any species of flora or fauna that is threatened with extinction throughout all or a significant portion of its natural range.

A *threatened form of life* is any species of flora or fauna that is likely to become endangered in Canada or Alberta if the factors affecting its vulnerability are not reversed.

A *vulnerable form of life* is any species of flora or fauna that is of concern because it is naturally scarce or likely to become threatened as a result of disclosure of specific information about it.

4.16 INFORMATION THAT IS OR WILL BE PUBLISHED

Overview

Section 28(1) provides that a public body may refuse to disclose information:

- that is available for purchase by the public (**section 28(1)(a)**); or
- that is to be published or released to the public within 60 days after the applicant's request is received (**section 28(1)(b)**).

Section 28 is a discretionary exception.

The provision enables a public body to refuse to disclose information that is currently available for purchase by the public. This allows the public body to follow its normal procedures for selling information, if its policy has been to do so, or to make a decision to publish particular information. The *Act* is not intended to replace existing procedures for access to information (**section 3(a)**).

It also provides for a public body to decide whether or not to withhold information that will be published or released within 60 days of the applicant's request.

Available for Purchase

Available for purchase by the public means that a publication is generally available for purchase from the public body or a government or private bookstore. It must be available to the general public, not only to a limited group such as realtors or an interest group (see *IPC Order 98-004*). **In such instances, the public body must tell the applicant where the publication may be purchased**.

Examples include maps, research reports, catalogues, and telephone directories.

About to be Published

There will be situations when a request is made for information that is about to be published. There may be a desire to claim the exception in **section 28(1)(b)** for a number of reasons. The publication may be required by the Legislature or a governing body, and the Minister or head cannot or will not release the information first through another channel. The public body may wish to control the date when the information is made public. As well, it may also be more convenient and economical to await the publication date.

The exception covers only the manuscript being published and not surrounding data or research and background material. These records will have to be dealt with separately, if requested, or if the applicant cannot be convinced that the request is satisfied by receipt of the publication.

Section 28(1)(b) may only be claimed if there are no legal impediments to publishing, such as **Part 2** of the *FOIP Act*.

The public body should have a copy of the information to which it is denying access readily available in order that it can be published or released in the requisite time frame. In order to claim **section 28(1)(b)**, the public body should have an active publication or release plan that establishes a date when the information will be available to the public.

The 60 days for publication or release is from the date of receipt of the applicant's request and not from the date when a response is made to the request.

It is important that a public body ensure that the requested records are either published or released to the public within the 60-day time frame established by the provision.

Released to the public means made available to the public at large either through active dissemination channels or through provision of the information at specific locations (e.g., public libraries).

Notification of Applicant

Section 28(2) requires the public body to notify an applicant of the publication or release of information that the head has refused to disclose under **section 28(1)(b)**.

Such notification should provide:

- the date of publication or release;
- the specific location where the applicant can have access;
- how access will be given;
- the purchase price, if this is relevant; and
- any other information that the public body is required to give the applicant under **section 11(1)** of the *Act*.

If there is no charge for the publication, the public body could simply provide a copy to the applicant on publication.

Failure to Publish

Section 28(3) states that if the information is not published or released within 60 days after the applicant's request is received, the public body must reconsider the request. This must be done as if it were a new request received on the last day of that period, and access to the information must not be refused under **section 28(1)(b)**.

This means that on the 60th day the public body is required to consider the applicant's request as a new request with 30 days to respond, dating from that day. The public body cannot employ the "publishing or release" exception in any consideration of the new request.

Chapter 5
Third Party Intervention and Notice

5.1 OVERVIEW

Many public bodies hold large quantities of information about individuals, companies, non-profit groups and other third parties. The *Act* recognizes that disclosure of this information might result in harm to these third parties (see Chapter 4.3 and 4.4). The *Act* provides for notification of third parties when access to records containing such third party information is requested.

A *third party* is defined in **section 1(1)(r)** as a person, a group of persons, or an organization other than an applicant or a public body. It includes individuals, sole proprietorships, partnerships, corporations, unincorporated associations and organizations, non-profit groups, trade unions, syndicates, trusts, and their legal representatives.

5.2 WHEN IS THIRD PARTY NOTIFICATION REQUIRED?

Section 29 of the *FOIP Act* applies when a request has been received for a record containing information that may be withheld under **section 15**, disclosure harmful to the business interests of a third party, or **section 16**, disclosure harmful to personal privacy.

Section 29(1) requires that a public body provide written notice to a third party when it is considering giving access to a record that may contain information described in **sections 15** and **16**. It is a *mandatory* provision.

This section does not apply to a record containing information described in section 16(2)(j). Disclosure of this information is not an unreasonable invasion of personal privacy. This allows for disclosure of personal information without having to locate individuals for notification.

It is important that public bodies take steps to allow individuals to request non-disclosure under section 16(3) when this personal information is collected, because third party notice will not be given in these cases.

Section 29(1) also does not apply when a public body invokes **section 28(1)** to respond to the request. **Section 28(1)** allows an exception to disclosure for information that is available through purchase, or will be published or released to the public within sixty days of receiving the request. As well, **section 29(1)** does not apply when a public body seeks advice from a third party about disclosure under another section of the *Act*. An example of this would be consultation with a federal government department under **section 20(2)**.

Section 29(2) provides that a public body may give written notice to a third party even though it intends to refuse access to records under **section 15** or **16**. This provision allows a public body to give a third party the opportunity to consent to disclosure of information that the public body intends to refuse to disclose. It also allows a third party that objects to disclosure of the information concerned to provide additional information in support of non-disclosure. This may be useful to a public body in defending its refusal to provide access before the Information and Privacy Commissioner.

The provision for notice to a third party when a public body does not intend to disclose third party information also permits a public body to provide notice to clients who may be third parties in an access request. The clients can be made aware that a request for information concerning them has been made before an applicant requests a review by the Information and Privacy Commissioner.

A public body can also provide a less formal notification, such as a telephone call. This might take place when a public body is very certain of its grounds for refusal of access and does not need representations from a third party to support this decision. Such an informal notice has no standing under the *Act* and is merely a courtesy to the third party.

Public bodies must ensure that they do not reveal the identity of the applicant in any communication, whether formal or informal, with a third party.

There is no obligation to undertake third party notice when a public body is intending to refuse access to information under section 15 or 16.

However, public bodies should note the Commissioner's comments on the merits of consulting with third parties, even when disclosure is not contemplated (see *IPC Order 97-018*).

An example of a third party notice given under **section 29(2)** is provided in **Model Letter K** in Appendix 3 of this publication.

5.3 HOW IS A THIRD PARTY NOTIFICATION PROCESS CARRIED OUT?

Section 29(1) requires that third party notice be given "where practicable and as soon as practicable." This means that third party notice must be given unless, after reasonable attempts to locate and notify the third party, it is impossible to do so. Such notice must be given as soon as possible in order to respond to the request within a reasonable time frame. Public bodies are expected to use only their own records and publicly available resources in trying to locate an address for a third party.

Notices must be in writing. **Section 29(1)** covers notice to the third party and **section 29(4)** states that, when a notice is given to a third party, a notice must also be provided to the applicant. **Where possible, these notices should be given at the same time.**

If more than one person or organization is affected by the disclosure of information in a record, a notice has to be given to each affected third party.

Section 78 requires that any notice or document to be given to a person under the *Act* be given:

- by sending it to that person by prepaid mail to the last known address of that person;
- by personal service;
- by substitutional service if so authorized by the Commissioner; or
- by means of electronic or other telecommunication messaging.

Public bodies should choose a delivery method that ensures that the notice arrives quickly and conveniently for the third party, but which is also efficient and cost-effective for the public body. Prompt delivery will allow the third party as much time as possible to respond.

Under normal circumstances, the public body sends notices to the third party and the applicant by mail (regular mail or priority post). Where possible and practical, a notice may be sent by fax, with originals following by mail. In exceptional circumstances, it may be necessary to send a notice by courier or registered mail.

If sending the notice by fax or other electronic means, care should be taken to prevent unauthorized disclosure of third party information. It may be necessary to telephone the third party before sending the notice to identify the individual best suited to deal with it or to advise of the electronic transmission.

Personal service means a method of delivery whereby it can be shown that the person to be served actually received the document.

Substitutional service means the placing of public notices in a trade journal or in other specialized or general media. This is normally intended for situations where a very large number of third party notices are required or where a third party cannot be located and the nature of the information would lend itself to this type of public notice.

When notice by substitutional service is contemplated, a public body should enter into a full consultation with the Office of the Commissioner about why it believes such notice is appropriate in the particular case. **Substitutional service can only be used with the permission of the Commissioner**.

5.4 CONTENT OF THIRD PARTY NOTICE

Section 29(3) states that a third party notice must:

- contain a statement that a request has been made for access to a record that may contain information the disclosure of which would affect the interests or invade the privacy of a third party;
- either include a copy of the record, or the part of it containing the information in question, or include a full description of the contents of the record involved; and
- contain a statement that, within 20 days after the notice is given, the third party may, in writing, either consent to the disclosure or make representations explaining why the information should not be disclosed.

A model letter, including the various options for third party notice, is set out as **Model Letter K** in Appendix 3 of this publication. The notice provides a summary of the particular exception involved (either **section 15** or **section**

16). It also provides an explanation of the points that a third party should address in any representations as to why information should not be disclosed. The version of this letter relating to **section 15** notes in particular the importance of providing clear and specific information relating to any harm that may be expected to result from disclosure of records to which **section 15** may apply.

Efforts should be made to ensure that the third party understands the significance of the notice, and also that only those matters pertinent to the applicability of **section 15** or **16** are relevant to the response. It must be clear that the public body cannot consider comments or statements on other exceptions when it makes its decision regarding the applicability of these exceptions.

The third party response must be in writing. A verbal response is not satisfactory for the purposes of section 29.

The identity of the applicant must not be included in the notice sent to the third party, unless the applicant has consented to this disclosure.

The notice must include the name, job title and telephone number of the person within the public body that the third party may contact for more information.

Good communication with the third party is a key to ensuring a smooth notification process and promoting better understanding of the third party's representations when determining the applicability of the exception.

5.5 NOTICE TO APPLICANT

Section 29(4) provides that, when notice is given to a third party, the public body must also provide a notice to the applicant.

The notice must state that:

- the requested record may contain information the disclosure of which would affect the business interests or invade the personal privacy of a third party;
- the third party is being given an opportunity to make representations respecting disclosure; and
- a decision whether or not to give access to the requested record(s) will be made within 30 days after the date of notice to the third party.

The identity of the third party is not included in the notice sent to the applicant.

A model notice to an applicant is included as **Model Letter L** in Appendix 3 of this publication.

5.6 RESPONSE FROM THIRD PARTY

In deciding whether or not to give access to all or a portion of the requested record(s), the public body must consider any third party responses received in reply to notices given under **section 29(1)** which are pertinent to **section 15** or **16**, as applicable.

Section 30(1) provides that a public body must decide whether or not to give access within 30 days of giving notice.

However, a decision cannot be made until the third party responds, or on the 21st day after notice is sent, whichever comes first.

Consent

If the third party consents to disclosure of the information, the public body releases the information unless another exception in the *Act* applies to it. The public body should be satisfied that the person giving consent to disclose information on behalf of a business or other organization is an officer, employee or corporate officer authorized to provide such consent.

Non-disclosure

If a third party makes representations as to why the information should not be disclosed, the public body considers the representations in reaching a decision on access. If there is any doubt that the third party has understood the significance of the notice or the criteria that apply in decisions regarding access, the public body should contact the third party by telephone to discuss the matter.

Non-response

If a third party does not respond to the notice within 20 days of the sending of the notice, the public body must make a decision based on the information available.

Failure to respond does not imply the third party's consent to the disclosure of the information. The public body must not draw any inference from the lack of a response.

Public bodies should contact the third party by telephone, fax or electronic mail to discuss why a response has not been made. The opportunity for contact extends up to the point of disclosure of the information. It may be helpful in the event of a review by the Commissioner for the public body to be able to provide documentation of its efforts to contact a third party.

5.7 NOTICE OF DECISION

Section 30(2) provides that once a public body has made a decision on access, it must give notice of this decision to both the applicant and the third party. This notice will vary according to circumstances.

When Access is Permitted

Applicant: The public body informs the applicant of the decision and the reason for it, and provides notice that access will be provided in 20 days if the third party does not ask for a review by the Information and Privacy Commissioner.

Third Party: The public body informs the third party of the decision and the reason for it, and provides notice that the third party can request a review of the decision by the Commissioner within 20 days after the date of the notice.

The public body cannot disclose the information until after the 20 days allowed for the third party to request a review.

When Disclosure is Denied

***Applicant*:** The public body informs the applicant of the decision and the reason for it, and provides notice that the applicant may, within 60 days, request a review of the decision by the Information and Privacy Commissioner.

***Third Party*:** The public body informs the third party of the decision and the reason for it, and advises that the applicant may, within 60 days, request a review of the decision by the Information and Privacy Commissioner.

Model Letters M and N in Appendix 3 of this publication cover the options for this type of notice.

5.8 TIME LIMITS

Section 10(1) states that a public body must make reasonable efforts to respond to a request within 30 calendar days of its receipt. The third party notification process allows the head of a public body to extend that time limit. Public bodies should not use this extension of time to unnecessarily delay responding to the applicant. Time extensions under **section 13** should be carefully considered (see Chapter 5.9 of this publication).

The major time limits are:

- third party notice is given as soon as possible, and, for the most part, within 30 days from the date the public body received the request;
- third parties have 20 days to respond to the notice;
- no decision can be made until this response is received, or 21 days after notice is given, whichever comes first;
- the public body must make a decision within 30 days after the notice is given (i.e., it has at least 10 days to consider the responses and make the decision);
- after notice of a decision is given, a third party has 20 days to ask for a review; and
- after notice of a decision is given, the applicant has 60 days to ask for a review.

It is not necessary to seek permission from the Commissioner for time extensions required to comply with the requirements of **section 30** with respect to the time allowed for the third party notification process and the time allowed for a third party to request a review.

The time limits for third party notice are set out in the flowchart contained in ***Figure 12*** at the end of the chapter.

Notice to Third Parties

This notice should be sent as soon as possible after the receipt of a request, and normally within 30 days of receipt of the request, unless the time limit has been extended for a reason other than third party consultation.

The 20-day time period allowed for a third party to respond to a notice begins on the day after the public body sends the notice, not the date the third party receives it. The date on which the notice is sent is the date marked on it indicating posting or electronic transmission (e.g., the postmark for regular mail, and the transmission date for e-mail or facsimile). For example, if a public body sends a third party notice by regular mail and the envelope is postmarked March 1, the third party has until March 21 to respond.

Response from Third Party

The third party has 20 days after the notice is given to respond, either by consenting to the release of the information or by making representations as to why the information should not be released.
If no response has been received by the 21st day after the notice was given, the public body decides, on the basis of the available information, whether or not to give access to the record.

Decision by Public Body

The public body is required to decide whether or not to give access to all or part of the record within 30 days after the third party notice is given.

Section 30(1) states that the public body may not make this decision until after the third party has had an opportunity to respond to the notice. Since the third party has up to 20 days to respond, the public body cannot make a decision on access until the earlier of:

- 21 days after the notice was given under **section 29(1)**; and
- the day a response is received from the third party.

Notice of Decision

By the 30th day after notice was given to the third party, the public body must give written notice of its decision regarding access to the record to both the applicant and the third party, but **it does *not* give immediate access to the record**.

Review of Decision

When the decision is to release all or part of the record(s), the third party has 20 days after the notice is given to ask the Information and Privacy Commissioner to review the decision. This 20-day period is calculated from the day after the public body gives the notice, not from the date the third party receives it.

It is important to note that the third party has only 20 days in which to request a review, not 60 days as allowed under **sections 63(2)** and **74(2)** in other instances.

This shorter period reflects the fact that the third party has already had time in which to prepare arguments on why information should not be disclosed.

Where the decision is to refuse all or part of the record(s), the applicant has 60 days to request a review in accordance with either **section 62(1)** or **73(1)**, as appropriate.

Access to Record

If the decision of the public body is to give access to a record or part of a record despite the representations of the third party:

- The public body must wait for a 20-day period after the notice of decision is given before the applicant is given access. This 20-day period allows the third party time to ask the Commissioner to review the decision.

- If the third party does not request a review within the 20-day period, the applicant is given access to the records that were the subject of third party representations on the 21st day.
- A public body may contact the Office of the Information and Privacy Commissioner to determine whether a request for review has been submitted.
- If the third party does request a review by the Commissioner, then the time limit for responding to the request is extended under **section 13(1)(d)**. The applicant is not given access to any record or part of a record that is the subject of the review until the review is completed. If the review affects only some of the records proposed for disclosure, the public body releases the remainder of the records to the applicant.
- The outcome of the review determines whether or not access is given to any record that is the subject of review.

The public body should provide the applicant with access to those records not affected by third party representations or subject to any other exception without waiting for the outcome of any consultation or review.

5.9 TIME LIMIT EXTENSION

If the third party notice is given early in the request management process and the third party responds promptly and has no objections to disclosure, the public body may be able to respond within the original time limit of 30 days from the receipt of the request, as allowed under **section 10**.

In most cases, more time will be needed for third party consultation. Generally, the period of 30 days after the date of notice (as allowed under **section 30(1)**) plus the period of 20 days for the third party to request a review (as allowed under **section 30(3)**) provides all the time necessary for the completion of the third party consultation process and no further extension is needed.

In some cases, however, additional time may be needed to complete third party consultations and make the decision on access. A public body may extend the time limit beyond

- the original 30-day limit allowed under **section 10**, or
- the longer period allowed under section **13(1)(a)** or **(b)**

to the extent required to enable the public body to comply with the requirements of **section 30** regarding third party consultation and right of review. Any longer extension must be requested in writing and approved by the Information and Privacy Commissioner.

Additional time may be needed in the following circumstances:

- the public body must consider a large number of third party representations; or
- the public body needs to consult further with third parties to clarify representations.

If possible, the public body makes the decision on whether or not an extension is needed when it gives notice to the third party and the applicant under **section 29**. If the public body cannot make an informed estimate of the time

required for third party consultations at the time notice is given under **section 29**, it may be necessary to delay the decision on extension until the responses have been received.
Situations may also arise where a public body has already claimed an extension (e.g., to process a large number of records) and then discovers third party information that requires a notice. The time for the third party notification process will carry the time beyond the 60-day limit that could be claimed through an extension by the public body under **section 13(1)**.

In such circumstances, the third party must have up to 20 days in which to make representations.

The public body would then extend the time limit to allow an additional 20 days for these representations.

A public body would also extend the time for response by 20 days after making a decision to disclose information in order to allow a third party to ask the Commissioner to review that decision.

If the third party requests a review by the Commissioner, the public body should consult with the Commissioner about the length of time needed for the review to take place.

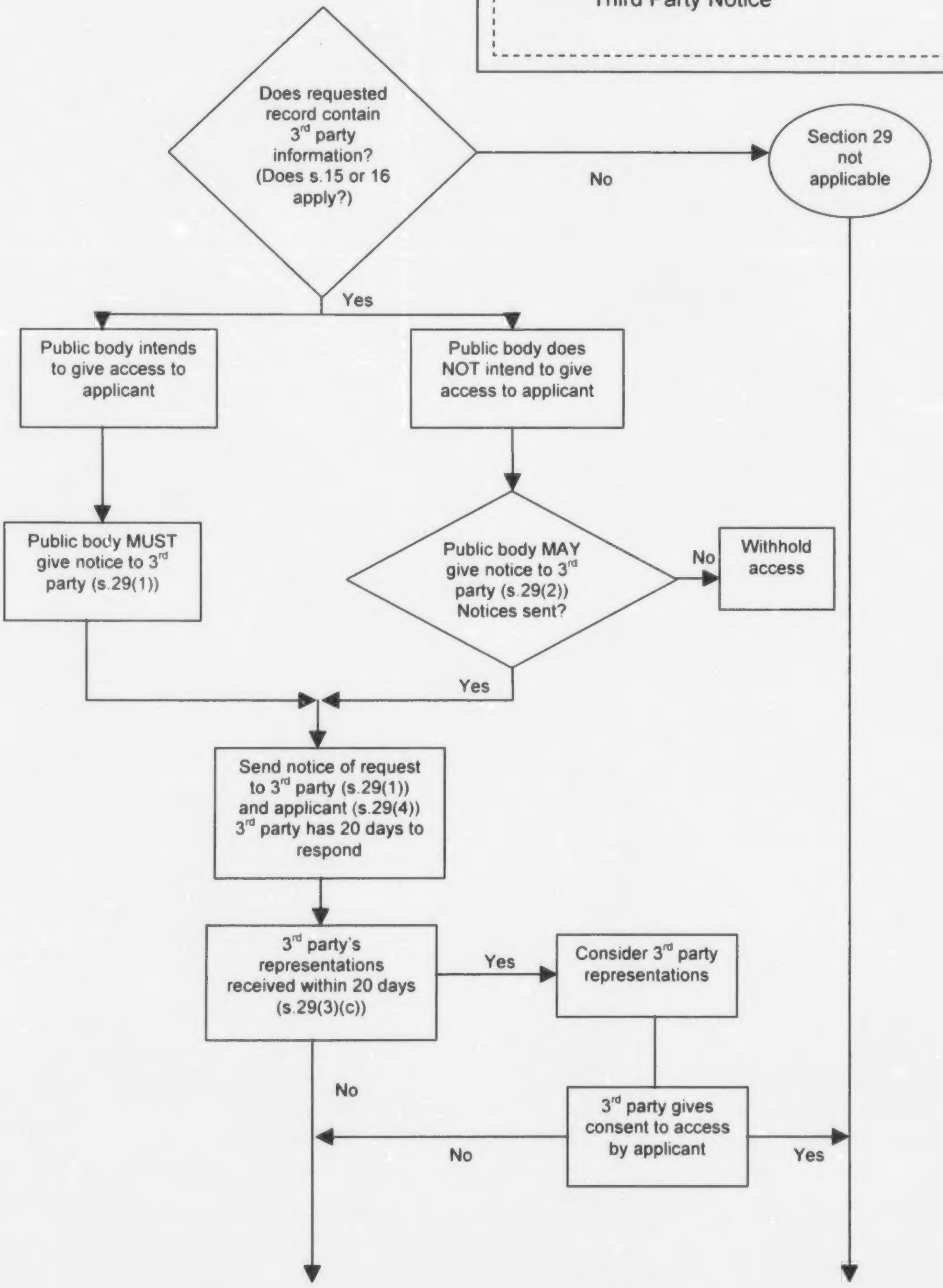
The applicant has the right to make a complaint to the Information and Privacy Commissioner about any time limit extension.

Application of Third Party Notice

Figure 12 contains a flowchart setting out the process for giving third party notice.

Figure 12

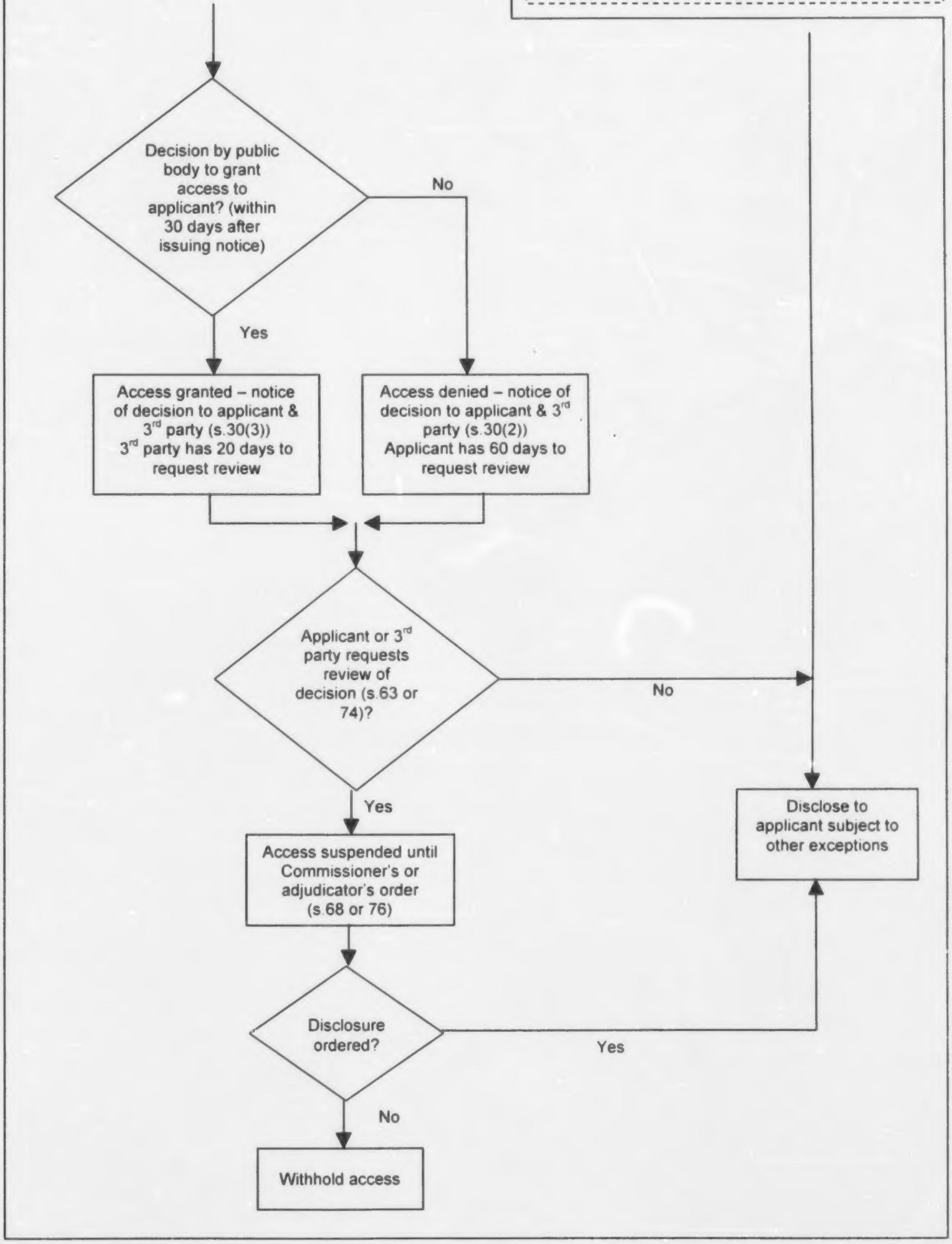
Sections 15 and 16 –
Third Party Notice


Does requested record contain 3rd party information? (Does s.15 or 16 apply?)
No
Section 29 not applicable
Yes
Public body intends to give access to applicant
Public body does NOT intend to give access to applicant
Public body MUST give notice to 3rd party (s.29(1))
Public body MAY give notice to 3rd party (s.29(2)) Notices sent?
No
Withhold access
Yes
Send notice of request to 3rd party (s.29(1)) and applicant (s.29(4)) 3rd party has 20 days to respond
3rd party's representations received within 20 days (s.29(3)(c))
Yes
Consider 3rd party representations
No
3rd party gives consent to access by applicant
No
Yes

...continued

Figure 12 – Continued

Sections 15 and 16 –
Third Party Notice


Decision by public body to grant access to applicant? (within 30 days after issuing notice)
No
Yes
Access granted – notice of decision to applicant & 3rd party (s.30(3)) 3rd party has 20 days to request review
Access denied – notice of decision to applicant & 3rd party (s.30(2)) Applicant has 60 days to request review
Applicant or 3rd party requests review of decision (s.63 or 74)?
No
Yes
Access suspended until Commissioner's or adjudicator's order (s.68 or 76)
Disclose to applicant subject to other exceptions
Disclosure ordered?
Yes
No
Withhold access

Chapter 6
Disclosure in the Public Interest

6.1 OVERVIEW

Section 31(1) of the *FOIP Act* establishes a public interest provision that obliges the head of a public body to disclose information without delay when:

- the information is about a risk of significant harm to the environment or to the health or safety of the public, a group of people, a person or the applicant; or
- the disclosure is, for any other reason, clearly in the public interest.

This provision applies whether an access request has been made or not. Disclosure may be to the public, to an affected group of people, to any person or to the applicant.

This is a *mandatory* provision. Any information that meets the criteria set out in the provision must be disclosed even if there has not been a formal request under the *Act*.

The provision further requires that action be taken *without delay*. The assumption is that any circumstances that would warrant consideration of **section 31** would be urgent, and that no delay should occur where disclosure is demanded by events that have an impact on public safety or where disclosure is in the public interest.

The circumstances may have developed over a period, but disclosure without delay may be required when the situation has reached a critical point.

The actual assessment of what constitutes *without delay* must be made on a case-by-case basis. Some factors that should be considered in the assessment are:

- the level of harm anticipated;
- the degree of risk that the harm will occur;
- the imminence of the harm, that is, whether there is a clear and present danger of significant harm;
- measures that could be taken to avoid the harm and the amount of time required for these measures, and whether release of information would likely reduce the risk of the harm;
- the importance of consulting with other public bodies whose interests may be affected by the disclosure;
- the right of a third party to make representations; and
- the right of the public to make informed choices about the risks to which they are exposed.

6.2 DISCLOSURE

Section 31 of the *Act* refers to *information* not *records*. Where a request for disclosure in the public interest is made by an applicant as part of a FOIP request, the decision of the public body will, most likely, be focused on particular records.

Where no FOIP request is made but the public body is considering disclosure in the public interest to the general public, an affected group of people or a person other than an applicant, the emphasis will almost always be on *information* as opposed to *records*. Disclosure might be of the facts surrounding an event or issue as opposed to the documents recording those facts (see *IPC Order 97-009*).

This distinction means that the public body might release only basic or summary information and not the whole record on an event, subject or issue that affects the public interest.

For example, a public body might release the location, nature and extent of the contamination of a building or site but not necessarily all the scientific, exposure, emergency response and property records that relate to the event.

Section 31 anticipates disclosure in four different ways:

- to the public generally;
- to an affected group of people;
- to any person; or
- to an applicant making a request.

Disclosure to the Public

Where the public interest dictates disclosure to the general public, the public body must ensure that the information is released in a manner designed to reach the public at large. Examples include the use of radio, television, newspapers, and electronic networks.

An example would be disclosure about an armed or dangerous criminal who is suspected to be in a particular area of Alberta. In this case, disclosure would be to the general public in that particular area.

Disclosure to an Affected Group

Where the information relates to circumstances that affect only a specific group of people, rather than the public at large, the head must ensure that effective ways are used to reach the affected group. If the information is of a sensitive nature, it is important that steps are taken to ensure that only the affected group is informed.

For example, if a safety hazard, such as an unstable trench, were discovered at a workplace, only those people on site who could come into contact with the hazard until it was fixed would need to be warned.

Disclosure to Any Other Person, including an Applicant

Where information relates to any other person, including an applicant, the public body must employ notification measures that provide the information to the person concerned and no one else, unless the public interest dictates wider disclosure of the information.

An example would be disclosure of the fact that an individual has been released on parole and continues to threaten the safety of his or her spouse.

In all cases, only the minimum amount of personal information necessary to alert the public concerned about the risk should be disclosed (see *IPC Investigation Report 98-011*).

6.3 PUBLIC INTEREST

Section 31 provides for disclosure in the public interest where the information is:

- about a risk of significant harm to the environment or to the health or safety of the public; or
- for any other reason, clearly in the public interest.

Risk of Significant Harm to the Environment or to Health and Safety

Risk is generally taken to mean the chance, possibility or certainty of danger, loss, injury or other adverse consequences.

The determination that there is a risk of harm to the environment or to public health or safety is usually made by professionals working for the public body or contracted by the public body to assess situations where there is a possible risk of harm. Determining the nature and extent of the risk is part of the management process.

Inclusion of the term *significant* in this provision means that the head of a public body must be convinced that the harm risked is considerably greater than in normal circumstances.

Harm to the environment refers to the damage to or degradation of any component of the earth, including air, land, and water; any layers of the atmosphere; and any organic and inorganic matter. It also includes damage to or degradation of the interacting natural systems that include components of these things, through either natural calamity or illegal or improper use.

An example might be information about toxic emissions from an industrial plant.

Harm to health means damage to the well-being of the body or mind of an individual, or the health of the general public. An example of a risk of significant harm to health might be the presence of contaminants or a virus in school or hospital buildings or contamination of a water supply.

Harm to safety means a condition where an individual or the general community does not feel safe and free from danger or risks. A risk of significant harm to safety might be created by a natural gas leak or a bomb threat that threatens an explosion in a populated area.

Section 31 of the *Act*, together with an Alberta Justice Protocol for the application of the provision, has been used to release personal information on the whereabouts of violent offenders released from correctional facilities who are still considered by law enforcement and parole officials as a serious risk to a community.

Public, Affected Group of People, Any Person or Applicant

Section 31(1)(a) applies to information that reveals a risk of significant harm to the general public, a specific group of people, or an individual, including an applicant.

Other Public Interest

Section 31(1)(b) is a general clause intended to cover any other situation where the head of a public body may decide that disclosure of information is in the public interest.

Such disclosure must be *clearly in the public interest*. This means that the case for release in the public interest is, in the opinion of the head, beyond reasonable doubt. The information involved must be a matter of compelling public interest and not just of interest or of curiosity to the public, a group of people, a person or the applicant.

6.4 DETERMINATION OF PUBLIC INTEREST

The determination of *public interest* will have to be made on a case-by-case basis and requires a balancing of the public interest in release of the information on the one hand and the public and private interests in protecting the information from disclosure on the other.

Examples where disclosure in the public interest might be considered are situations where:

- a public body has been alerted about a contagious disease or about an individual who is the carrier of a contagious or dangerous disease;
- a violent or dangerous offender has been released into the community;
- an individual seeking employment in child care on the basis of a false resume is found to have a history of child molestation that is recorded in a register of employment references for child-care workers; and
- information has come to light about corruption or serious misuse of public funds.

These are only illustrative examples where the public interest *might* be involved and situations will have to be judged on a case-by-case basis.

The burden of proof lies with the public body to show that **section 31** ought *not* to be applied since it has a positive obligation to apply it where necessary.

In determining whether or not an issue is *clearly in the public interest*, reference should be made to *IPC Order 97-018* (which summarizes *Adjudicator's Order 96-014* and *IPC Order 96-011*) and *IPC Order 98-019*. The Commissioner has noted that the Legislature did not intend **section 31** to operate simply because a member of the public asserts "interest" in the information. The condition that disclosure of the information must be *clearly in the public interest* means that the information must relate to a matter of compelling public interest. This will be judged on a case-by-case basis.

Public bodies may wish to consider in advance the conditions or criteria that might be typical of their programs where **section 31** would be considered. It is recommended that a senior official in the public body retain the authority for decisions on **section 31**. Examples include a Deputy Minister in a government department or the Chief Administrative Officer of a regional health authority.

6.5 SCOPE

Section 31(2) provides that this section of the *Act* overrides all other sections of the *Act*.

This means that, if there is a risk of significant harm to the environment or to public health or safety, or disclosure is clearly in the public interest (**section 31(1)**), a public body must disclose information, including essential personal information, despite:

- the exception to disclosure of information harmful to personal privacy in **section 16** of the *Act*; and
- the privacy protection provisions relating to disclosure of personal information in **section 38**.

The public interest disclosure provision represents a very significant exception to the rules for privacy protection, and any disclosure under **section 31** of the *Act* should be carefully considered and justified (see *IPC Investigation Report 98-011*).

6.6 NOTIFICATION

Section 31(3) provides that, before disclosing information under **section 31(1)**, the public body must, if practicable:

- notify any third party to whom the information relates;
- give the third party an opportunity to make representations; and
- notify the Commissioner.

Normally, notice must be given to affected third parties and the Information and Privacy Commissioner *before* the information is released under **section 31(1)**.

However, this obligation to notify third parties and the Commissioner must be balanced against the obligation to disclose the information without delay. Notification is to take place only *where practicable*, and the head of the public body must ensure that there is no delay adversely affecting the public interest. The factors governing release *without delay* outlined in section 6.1 of this chapter also apply here.

Such notice should take a similar form to the notice required by **section 29(1)** of the *Act*. Given the urgency of the situation, it should be delivered by fax or courier and accompanied by a telephone call advising the third party of the importance of making any representations by similarly expeditious means. Depending on the urgency, the third party may be asked to respond immediately or may be given a period of time.

Model Letter O in Appendix 3 of this publication covers this type of situation.

The third party notice should be sent to any person, group of persons or organization, other than the person who made the request or a public body, that is a subject of the information or the record(s).

A similar notice, or a copy of the one sent to the affected person together with a covering note, must be sent to the Information and Privacy Commissioner to inform that office that a disclosure in the public interest is being made.

Section 31(4) requires that, where notification is not practicable under **section 31(3)**, the public body must mail a notice of disclosure:

- to the last known address of the third party or parties; and
- to the Commissioner.

Model Letter P in Appendix 3 of this publication can be used in this situation. A copy of the letter and a covering note can serve as notice to the Information and Privacy Commissioner.

6.7 REVIEW

If there is a complaint about the failure of a public body to release information in the public interest, the Information and Privacy Commissioner can review the head's decision:

- *if a FOIP request has been made*, under the powers provided in **section 62(1)** of the *Act*, which enables an applicant to request a *review* of the decision and prescribes a process for this to occur; and,
- *if no FOIP request has been made*, under the general powers of the Commissioner set out in **section 51(1)** of the *Act*, which permits an *investigation* of various matters relating to the legislation.

The powers of the Information and Privacy Commissioner are discussed in more detail in Chapter 10 of this publication.

IPC Order 96-011 discusses the powers of review and investigation of the decision of the head of a public body in dealing with disclosures under **section 31**.

In that order, the Commissioner clearly indicated that a person will have to approach the head of a public body to request disclosure in the public interest. The Commissioner may review or investigate a decision of the head to disclose or not to disclose information under **section 31**, but only to the extent of deciding whether discretion has been exercised properly and whether the decision is rationally defensible. The Commissioner will not substitute his view for that of the head as to whether the decision the correct one.

6.8 DISCLOSURE TO THE COMMISSIONER

Section 77(1) of the *Act* provides that an employee of a public body may disclose to the Commissioner any information which that employee is required, whether under oath or by agreement, to keep confidential, if the employee, acting in good faith, believes that the information:

- ought to be disclosed by the head of the public body under the public interest provisions of **section 31**; or
- is being collected, used or disclosed in violation of the privacy provisions contained in **Part 2** of the *Act*.

The Commissioner will seek proof that the employee is acting in *good faith*. This means that the employee has an honesty of intention or honestly believes that he or she is following a lawful path.

If the Commissioner is satisfied that the complaint is in good faith, there must be an investigation of the disclosure. The investigator may use all the powers vested in the Office of the Commissioner to investigate the matter (**section 77(2)** and **(7)**).

The Commissioner is forbidden to divulge the identity of the employee except with that individual's consent (**section 77(3)**).

Disclosure can occur through written communication with the Commissioner or through a meeting between the employee and the Commissioner or one of the Commissioner's staff delegated to undertake the case.

If an employee acted in good faith, he or she is protected from prosecution under any Act for:

- copying a record or disclosing it to the Commissioner; or
- for disclosing information to the Commissioner (**section 77(4)**).

An employee acting in bad faith would not be protected from prosecution.

Bad faith means acting with mischievous, harmful or false intent.

A public body or any person acting on behalf of a public body is prevented from taking any adverse employment action against an employee acting in good faith who:

- has disclosed information to the Commissioner under this section; or
- has exercised or *may exercise* a right under this section (**section 77(5)**).

Any person who violates the principles and rights set out in **section 77(5)** is guilty of an offence and liable to a fine of not more than $10,000 (**section 77(6)**).

The intent of the section is to give balanced and adequate protection to employees. This is to encourage employees to come forward when they honestly believe that the public body for which they work is:

- either ignoring an important public interest in failing to release particular information; or
- is failing to meet the obligations to protect personal privacy imposed by the provisions of **Part 2** of the *FOIP Act*.

Chapter 7
Protection of Privacy

7.1 OVERVIEW

Part 2 of the *FOIP Act* establishes conditions and obligations that public bodies must meet in protecting the privacy of individuals whose personal information is in their custody or under their control. The provisions are based on the international privacy standard issued by the Organization for Economic Cooperation and Development (OECD) and commonly known as the OECD Privacy Guidelines. Canada became a signatory to this standard in 1984.

These OECD Guidelines were used as the basis for the development by the Canadian Standards Association of the *Model Code for the Protection of Personal Information* (CAN/CSA-Q830-96). The *FOIP Act* is generally consistent with the principles set out in the *Model Code*. While the *Model Code* does not apply to public bodies, it has been adopted voluntarily by a number of private-sector organizations and forms the basis of the proposed federal *Personal Information Protection and Electronic Documents Act*.

Sections 32 to 41 of the *Act* establish controls over the collection, use and disclosure of personal information and requirements for protecting, correcting, retaining, and ensuring the accuracy of the information.

Personal information is recorded information about an identifiable individual. The extent and nature of personal information is defined in **section 1(1)(n)** of the *Act*. This definition is included in Appendix 1 of this publication, **Definitions.**

The provisions relate to *all* personal information in the custody or under the control of public bodies, *except* for personal information that is outside the scope of the legislation (see Chapter 1.7 of this publication on exclusions from the *Act* and the effect of paramountcy).

Public bodies that hold personal information to which the *Act* does not apply should bear in mind that it is good business practice:

- to inform individuals about the purpose of collecting their personal information;
- to take steps to ensure the accuracy of personal information; and
- to protect personal information from unauthorized access, use or disclosure.

Public bodies collect and retain information for a variety of purposes that are essential to their effective and efficient operation.

The FOIP legislation requires public bodies to balance operational efficiencies against the interests of individuals in their own information and privacy. This balance is achieved by good information management practices, including controls over the collection of information by public bodies, the disclosure of information for a variety of public purposes, and electronic information system design. These privacy protection measures are often referred to as a *code of fair information practices*.

The *Act* provides that public bodies must:

- give individuals access to their own personal information and the opportunity to request correction of errors or omissions in it;
- collect personal information only for purposes authorized under an enactment, for law enforcement, or when needed to operate programs or for other activities;
- collect personal information directly from the individual concerned unless the individual authorizes collection from another person, or the *Act* authorizes indirect collection;
- notify individuals about the authority for and purpose of collecting their personal information unless such notification will lead to the collection of inaccurate information;
- use and disclose personal information only for the purpose for which it was collected, for a consistent purpose, or for a purpose set out in the *Act*;
- make reasonable efforts to ensure that the personal information they collect for decision-making purposes is accurate and complete;
- retain personal information used for decision-making purposes for at least one year after it has been used so that individuals may exercise their rights of access and correction; and
- make reasonable security arrangements to protect personal information in their custody or under their control.

Part 2 of the *Act*, Protection of Privacy, may be best implemented if the FOIP Coordinator ensures that close cooperation occurs with program directors or managers responsible for personal information holdings, the Senior Records Officer and the head of Information Technology, in organizations where these centres of responsibility exist.

It is important to understand **Part 2** of the legislation in relation to **Part 1,** Freedom of Information. **Part 1** deals with the access process under the *Act* when an applicant submits a FOIP request. **Part 2** addresses the manner in which personal information must be handled by public bodies at all times.

Part 1 establishes a right for individuals to access information about themselves (**section 6(1)**), and this is complemented in **Part 2** by the right to request correction of that personal information (**section 35**).

Part 1 also incorporates, in **section 16**, a balancing test to determine whether or not release of personal information would be an unreasonable invasion of personal privacy. This test comes into play whenever an applicant other than the individual the information is about, or that individual's personal representative, makes a request for a record containing personal information.

For more information on the exception for disclosure of information harmful to personal privacy, see Chapter 4.4 of this publication.

This provision is complemented by **section 38,** which applies, in the absence of an access request, to regulate the disclosure of personal information to parties other than the individual the information is about. **Section 38** governs disclosure of personal information both in response to external requests and in the internal business activities of public bodies.

Part 2 applies equally to public bodies and to persons, groups and organizations acting on behalf of a public body under contract. **These contracts must stipulate clearly the privacy requirements of the *Act* imposed on the public body and ensure the contractor assumes them.**

For further information on the application of the *Act* in the contracting process, see the publication *Freedom of Information and Protection of Privacy: Contract Manager's Guide*, produced by Information Management and Privacy, Alberta Municipal Affairs.

7.2 PURPOSES OF COLLECTION

Section 32 of the *Act* provides that no personal information may be collected by or for a public body unless:

- the collection of personal information is expressly authorized by or under an enactment of Alberta or Canada;
- the personal information is collected for the purposes of law enforcement; or
- the personal information relates directly to and is necessary for an operating program or activity of the public body.

Collection occurs when a public body gathers, acquires, receives or obtains personal information. It includes activities where individuals respond through interviews, questionnaires, surveys, polling, or by completing forms in order to provide information to public bodies. There is no restriction on how the information is collected. The means of collection may be writing, audio or video taping, electronic data entry or other such means.

Section 32 of the *Act* stipulates that collection can take place *by or for* a public body. A public body is bound by the requirements of the *Act* whether it conducts its own collection activities or authorizes an outside agent to carry out the collection. This authorization may be either under contract or through an agreement or arrangement with another public body or private organization.

Examples of organizations and individuals that might collect personal information on behalf of a public body include non-profit support groups such as the John Howard Society, medical laboratories and diagnostic imaging firms, and school counsellors.

When collection of personal information is carried out by one public body on behalf of another public body, this must be done under a written agreement. The agreement should state the reasons for collecting information in an indirect manner, the specific authority for the collection, and the purposes for which the personal information will be used or disclosed. Any use or disclosure of the personal information must be authorized under the *Act* (see *IPC Investigation Report 99-001*).

When an outside organization or contractor is collecting personal information on behalf of a public body, the public body must have in place a written agreement or contract. This must stipulate how the organization or contractor will meet the requirements of the *Act* regarding the collection, use, disclosure, security, retention and disposition of the personal information being collected.

Section 32(a) provides that collection may be expressly authorized by an enactment of Alberta or Canada. This means that collection may find its authority in either provincial or federal statute or provincial or federal regulations.

In some Acts, there is detailed provision for the collection of certain specific types of personal information. In these cases, the statute both authorizes collection and identifies the personal information that can be collected. More commonly, the Act will authorize a program or activity, and a regulation under the Act will provide detailed authority for collection and sometimes the format in which the information is to be collected. An example of this form of authorization for collection is the *School Act* and the Student Record Regulation.

If an enactment authorizes a program or activity, but there is no specific authorization for the collection of information for the purposes of the program or activity, a public body cannot rely on the enactment as authority for collection of the information.

Section 32(b) permits the collection of personal information for the purposes of law enforcement. *Law enforcement* is defined in **section 1(1)(h)** of the *Act* and further explained in Chapter 4.7 of this publication.

Section 32(b) recognizes that law enforcement agencies must engage in wide-ranging information collection that would not always be allowed under the more restrictive terms of **section 32(c)**.

It would be difficult for a law enforcement agency to show, at the moment of collection, how each piece of personal information collected for investigative or enforcement purposes relates directly to or is necessary for the activity under way. Certain investigative methods, such as taking witness statements, might be seriously compromised by limiting the collection of personal information.

Section 32(c) permits the collection of personal information when that information

- relates directly to, and
- is necessary for,

an operating program or activity.

Most often, legislation will only give authority for a particular program or activity, without authorizing the collection of specific personal information. Public bodies must then determine the exact elements of personal information which they need to administer a particular program and design collection instruments to obtain this information *and no more*. Collection authority then derives from **section 32(c)** of the *Act*.

Relates directly to means that the personal information must have a direct bearing on the program or activity.

Necessary for means that the public body must have a demonstrable need for the information.

The word *and* is restrictive. The collection must meet both parts of the two-part test in order for the public body to use **section 32(c)** as authority to collect personal information.

For example, if a program provides a particular benefit or service, information will be needed to ensure that an individual is eligible or qualified for that benefit or service. Personal information not related to the particular benefit or service is not required and should not be collected, even though it may be potentially useful to another program in the same public body.

An *operating program* is a series of functions designed to carry out all or part of a public body's operations. An *activity* is an individual action designed to assist in carrying out an operating program.

An important part of administering **section 32** involves public bodies undertaking a regular review of their current collection of personal information to ensure that it meets one of the three purposes discussed above.

Such a review should:

- seek to clarify authorizations for collection of personal information;
- eliminate any collection of personal information that does not meet the criteria set out in **section 32** and amend collection instruments, contracts and agreements, and policies and procedures that require the collection of this personal information;
- ensure that information that is needed for subsets of clients is collected *only* for those clients (see *IPC Investigation Report 98-003*);
- implement administrative controls that continue to ensure that all new or modified collections of personal information meet the criteria set out in **section 32** and ensure that the minimum personal information necessary to meet program needs is collected; and
- implement administrative controls to ensure that any irrelevant personal information that is sent to a public body is placed in a separate file so that it is not improperly used, and that it is destroyed at an appropriate time after completion of the process for which the information was inadvertently collected (see *IPC Order 98-002*).

This review should be carried out by the program areas having custody or exercising control over personal information, with the advice and cooperation of the FOIP Coordinator.

Administrative controls can be established in privacy standards, which should be included in the policy governing the overall collection activities of a public body. New collection activities and instruments should be reviewed by the FOIP Coordinator's office.

The review may be carried out in conjunction with reviews of information management practices and systems, which are discussed in Chapter 9 of this publication.

7.3 MANNER OF COLLECTION

Section 33(1) states that, subject to some limited exceptions, a public body must collect personal information directly from the individual the information is about. This establishes direct collection as the primary method for obtaining personal information.

This is an important principle of fair information practices. It helps to ensure that an individual is aware of the type of personal information being used to make a decision concerning him or her.

A public body must not, unless it is authorized to do so in the exceptions to this provision, seek the information from another source, even though it may have the capability of doing so.

Exceptions to Direct Collection

The *Act* provides for a number of circumstances where personal information about an identifiable individual may be sought from sources other than the individual the information is about.

Another method of collection authorized by the individual concerned, another Act or regulation, or the Commissioner **(section 33(1)(a)):** This provision allows another person or organization to provide personal information about an individual under one of the specified conditions. If the provision applies, information may be provided orally, through written correspondence, electronic information exchange or file transfer.

When an individual authorizes the collection of his or her personal information from another source, this authorization should be in writing. This may take the form of a signed authorization on an application form or a letter giving authorization.

If authorization is less formal, as in a case where an individual provides authorization orally over the telephone, the public body should document the conversation and, whenever possible, send a letter to the individual concerned setting out what he or she has consented to.

When asked to consent to indirect collection of personal information under **section 33(1)(a)(i)**, the person should be informed of:

- the nature of the personal information to be collected;
- the purpose of the indirect collection;
- the reasons for making the collection indirectly; and
- the consequences of refusing to authorize the indirect collection.

Sometimes another Act or regulation under another Act specifically authorizes indirect collection of personal information. Examples include the *Workers' Compensation Act* and the Alberta Health Care Insurance Regulation.

The Information and Privacy Commissioner has the power to authorize indirect collection under **section 51(1)(h)**. This provision addresses situations where indirect collection should be considered but **section 33** does not permit it. The Commissioner has the responsibility of deciding how and under what circumstances his powers in this regard will be exercised.

Information that may be disclosed under Division 2 of Part 2 of the Act (use and disclosure of personal information) **(section 33(1)(b)):** This provision permits a public body to collect personal information from a second public body, rather than from the individual the personal information is about, where the second body is authorized to disclose such information under **sections 37 to 40** of the *Act*. **Section 33(1)(b)** provides the connection between use and disclosure on the one hand, and indirect collection on the other.

Where public bodies rely upon this provision to collect personal information indirectly, the public body that has the information must be satisfied that the disclosure is authorized. The public body receiving the information must ensure that it has authorization to collect it under section 32.

This provision recognizes the legitimate sharing of personal information between public bodies in limited and controlled circumstances, and the fact that more than one public body may need exactly the same personal information. It reduces the burden on the public to provide information to public bodies, as well as the cost of collecting personal information to operate programs and activities.

Information collected in a health or safety emergency **(section 33(1)(b.1)):** This provision allows emergency services personnel, as well as other employees of a public body, to collect information needed to deal with an emergency situation.

This can happen when:

- the individual is not able to provide the information directly; or
- direct collection could reasonably be expected to endanger the mental or physical health or safety of the individual or another person.

Examples of such emergency situations include cases were an injured person is not able to respond to questions about medication; accident or fire situations when a delay in collecting information about a person's actions could result in death or severe complications; cases where an unconscious person is suspected of having a communicable disease; and cases where treatment information is required from a physician or pharmacist.

Only information needed to deal with the emergency should be collected indirectly.

Information about an individual who is designated as a person to be contacted in an emergency or other specified circumstances **(section 33(1)(b.2)):** This provision allows for the collection of the name, relationship, address and telephone number(s) of an emergency contact. The individual may be a family member or a friend. Normally this information would be collected from the individual who is required to provide an emergency contact.

Such information is often provided when, for example, students enter a college residence, children are registered in a day camp program or for a school field trip, or a public body hires a new employee.

***Information collected for the purpose of determining suitability for an honour or award* (section 33(1)(b.3)):** This provision allows a public body to seek references and other personal information about someone being considered for an honour or award. This includes honorary degrees, scholarships, prizes, and bursaries.

The nature of some awards is such that the potential recipients do not have to apply for the award and may not be aware that they are being considered. Scholarships and bursaries are often awarded on the basis of academic achievement and recommendations by faculty members; honorary degrees are usually awarded in recognition of a person's contribution to a community or sector of society; and prizes may be awarded on the basis of athletic or scholastic achievements.

Any information collected should be directly related to the honour or award being bestowed. Once the individual has been informed about the honour or award, he or she should be asked to consent to any future disclosure of personal information collected in connection with the honour or award.

***Information collected from published or other public sources for fund-raising* (section 33(1)(b.4)):** This provision allows for limited collection of publicly available personal information without the consent or knowledge of an individual. The information collected can be used only for fund-raising purposes.

Public bodies should keep such information segregated in their records and allow access by only those employees engaged in fund-raising and fund development activities.

Published sources are those that are normally available in print form or in some other generally accessible form such as audio tapes or video tapes.

Examples include newspaper reports, clipping files, corporate reports of public companies, and articles in periodicals. Most of this information would be readily available in a public or specialized library.

Other public sources includes information that is generally available to the public, either free or for a fee, but is not necessarily published in a commercial format or as a matter of course.

Examples include information available on the Internet, information in reports of charitable organizations, announcements of honours or awards granted by or through a public body in Alberta, and copies of speeches or speaking notes when the speeches are given at a public event.

Not included under this provision is information of a more private character, such as information based on personal acquaintance, friendship or observation that may be provided by members of a governing board or employees, information that could only be gathered through surveillance or from private sources, patient or next-of-kin information, or names of parents of students.

For more information on this provision, see *FOIP Bulletin No. 5, Fund-Raising.*

***Information collected for the purpose of law enforcement* (section 33(1)(c)):** This provision allows law enforcement bodies to collect personal information indirectly when it is needed in investigations. It is obvious that a law enforcement body will not always collect information about a suspect only from the suspect him or herself.

Much personal information about a person who is under investigation is collected from other sources. Reasons for this include the fact that investigators may not wish to alert the individual concerned that an investigation is taking place, the individual would not provide accurate information, or the individual might alter or destroy evidence. See Chapter 4.7 of this publication for information on the definition of law enforcement.

***Information collected for the purpose of collecting a fine or debt owed to the Government of Alberta or a public body* (section 33(1)(d)):** This provision allows either a representative of the provincial government, as a whole, or of any individual public body to contact any person or organization that may be able to help in the collection of money owed to the public body or the government. This may include finding the home or work location or telephone number of the individual who owes money.

A *debt* is something that is owed, usually money, where the individual has an obligation to pay and the creditor has the right to receive and enforce payment.

A *fine* is a monetary punishment imposed on a person who has committed an offence, including an offence under a by-law.

When public bodies face the problem of not being able to locate those owing money, or when they believe they would not obtain accurate information needed to collect the debt from direct sources, they are permitted to collect personal information from other sources.

***Information concerning the history, release or supervision of an individual under the control or supervision of a correctional authority* (section 33(1)(e)):** This provision permits correctional and parole authorities to seek out information from a variety of sources about individuals under their control or supervision. The individuals may be in a correctional institution or may be supervised in the community.

History here means information about the person's background, including employment record, medical condition and behaviour.

Release includes both permanent and temporary release from a correctional institution.

Supervision includes any community disposition requiring supervision of an offender, including probation, bail supervision, parole, temporary absence, and ordered community service work, as well as supervision of an individual held in a correctional institution.

***Information collected for use in the provision of legal services to the Government of Alberta or a public body* (section 33(1)(f)):** This provision recognizes that lawyers representing the provincial government or a public body may have to collect personal information to perform their jobs. The information may be required for day-to-day provision of legal services, or in the preparation for a proceeding before a court or tribunal.

Very often the nature of such activities precludes direct collection of the personal information because inaccurate information may be given. It may also be desirable that legal inquiries be made in confidence, or it may be that the individual concerned may not be able to provide the required information. In these circumstances the public body's legal representatives, or others providing legal services, can collect information indirectly, or ask an employee to do so on their behalf.

***Information necessary to determine eligibility to participate in a program or receive a benefit, product or service from the Government of Alberta or a public body and collected in the course of processing an application by the individual the information is about* (section 33(1)(g)(i)):** This provision recognizes that many programs operated by public bodies have eligibility criteria that must be met in order for an individual to participate in them or receive a benefit or service. This may require the public body to approach several different sources of information besides the individual to determine whether the criteria or qualifications are met.

Examples include verification of income for the Alberta Seniors Benefit, low-income housing or other income-tested programs; verification of assets for programs requiring asset testing; and verification of educational prerequisites for a post-secondary program.

This collection of information can only take place in the course of processing an application from the individual, or from his or her representative. It is good business practice to inform the individual about whom information is being collected that information from a variety of sources will be collected to document a particular application. A statement of consent, signed by the individual, can be included on the application form.

The program, benefit, product, or service may be one offered on behalf of the provincial government or may be specific to a particular public body.

***Information necessary to verify eligibility to participate in a program of or receive a benefit, product or service from the Government of Alberta or a public body and collected for that purpose* (section 33(1)(g)(ii)):** This provision is intended to allow for cases where an individual has already qualified for a program, benefit, product, or service and a public body needs to check to determine whether the eligibility remains valid.

In this case, personal information may be collected from a variety of sources other than the individual the information is about, and the individual may not be informed that verification is taking place.

For example, random checks of sources of information on the income and assets of individuals on social assistance or in low-income housing may be made to determine whether or not an individual remains eligible for the program. Such a check may involve an interview with the individual but may also involve collection of personal information about an individual from other sources. Another example would be verification of a student's continued enrolment in a program in order that the student may continue to receive student financial assistance or a grant.

As with the previous provision, it is good business practice to inform the individual about whom the information may be collected that verification of continuing eligibility may occur without notice. This is especially the case if the individual may incur any penalty for receiving a benefit for which he or she has become ineligible.

***Information collected for the purpose of informing the Public Trustee or the Public Guardian about clients or potential clients* (section 33(1)(h)):** The *Public Trustee* is the trustee for dependent adults who are unable to administer their own financial affairs because of a mental disability. The Trustee also administers the estates of persons who die intestate if the deceased persons have no adult beneficiaries residing in the province.

In addition, the Trustee acts as guardian by protecting the assets and financial interests of missing persons and children under 18 years of age.

The *Public Guardian* is charged with the responsibility of ensuring that appropriate surrogate decision-making mechanisms, supports and safeguards are available to assist adults who are unable to make personal decisions independently.

This provision permits personal information to be collected indirectly from relatives, friends and others about anyone who is or may become a ward of the Public Trustee or Public Guardian. This may include information about the individual's mental or physical health, financial information, employment or educational history, and opinions about the individual.

***Information collected for the purpose of enforcing a maintenance order under the Maintenance Enforcement Act* (section 33(1)(i)):** This provision permits Alberta Justice to collect personal information about a separated or divorced spouse under certain circumstances. Where information cannot be gathered directly from an individual who has defaulted on maintenance support payments – because that person either cannot be located or is resisting the court order for maintenance – information may be collected from public bodies and other sources. This allows the Department to locate the defaulting spouse and enforce a maintenance order set down by a court.

***Information collected for the purpose of managing or administering personnel of the Government of Alberta or the public body* (section 33(1)(j)):** This provision allows government departments and public bodies subject to the *Public Service Act* to collect personal information about an employee or potential employee from sources within the Government of Alberta. The provision recognizes the provincial government as the employer for all provincial departments.

Section 33(1)(j) also allows public bodies to collect information about employees or potential employees from third parties. Any collection under this provision must have, as its purpose, the management or administration of the personnel of the public body collecting the information.

Management or administration of personnel includes all aspects of the management of human resources of a public body, including the government-wide network managed through the Personnel Administration Office. It includes staffing, job classification, recruitment and selection, salary, benefits, hours and conditions of work, leave management, performance review, training, separation, and layoff. It does not, however, include management of consultant, professional or other personal services contracts.

Employees should be informed in a general way as to how personnel information about them is collected and from what sources they can expect this information to be derived. They should also be aware of the purposes for which various types of information are used and of their rights under the *Act*.

Examples of such collection include the collection of references for potential employees, determination of qualifications and performance for secondment and training opportunities, and the provision of pay and benefit services by one public body for other public bodies.

This provision refers to official personnel activities and does not sanction the collection of personnel-related information by individual officials for purposes other than official duties relating to the management and administration of personnel within a public body.

***Information collected for the purpose of assisting in researching or validating the claims, disputes or grievances of aboriginal people* (section 33(1)(k)):** This provision permits a public body to collect personal information indirectly in order to research the background and expedite the settlement of wider rights of aboriginal people.

Validating means confirming rights that have been contended by the parties to a claim, dispute or grievance.

The term *claims, disputes and grievances* is interpreted broadly to include all manner of controversies, debates and differences of opinion regarding issues in contention and is not restricted to differences over land claims.

Aboriginal people means individuals whose racial origins are indigenous to Canada.

Notification

Section 33(2) sets out rules that a public body must follow when it is required to collect personal information *directly* from an individual. A public body must inform the individual of:

- the purpose for which the information is collected;
- the specific legal authority for the collection; and
- the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

The requirement to provide notification applies only in those situations where information is collected *directly* from an individual.

The requirement to notify recognizes the individual's right to know and understand the purpose of the collection of personal information and how the information will be used. It also allows the person to make an informed decision as to whether or not to give personal information when there is no statutory requirement to do so.

Examples of cases where collection of personal information requires notification under this provision include collection of personal information on a client survey, collection of health information for use by nurses in a post-secondary institution in case of an emergency, and collection of individually identifying information on a course evaluation form.

Notification may given in many ways. It may be:

- printed on a collection form;
- contained on a separate sheet or in a brochure accompanying a form;
- published in a calendar of a post-secondary institution or an information brochure about a program;
- displayed on a notice hung on the wall or placed on a service counter; or
- given verbally.

A notification, consisting of the three elements set out in **section 33(2)**, should appear on or accompany all forms used to collect personal information directly from individuals. The same form of notice is required for computer-generated forms, regardless of whether an employee of the public body enters the information about the individual or the individual does the entry.

Notice should be given to individuals at the beginning of an interview when an individual is being asked to provide his or her own personal information. If the interview is being recorded, it is good practice to record the notice at the beginning of the tape.

When individuals are applying for and participating in extensive and complementary programs, it may be more convenient and effective to place a generic notice in a publication about the programs, or explain orally. However, it is important that the individual is given an opportunity to make an informed decision as to whether or not to give the information and understand any consequences that may result from not doing so, including any limitations on services that the public body may provide in the absence of the information. This applies when information is collected over the telephone as well as in other cases.

When a notification is given verbally, either in person or over the telephone, care should be taken to ensure that the individual is informed of the privacy requirements in the *Act*. An explanatory document can be provided either at the counter or later by mail. It is also good practice to provide written confirmation of telephone collection of personal information.

It is good for a public body to provide an applicant with a copy of the notice and to retain a copy on file.

The *purpose* of a collection means the reason for which the information is needed and the use(s) that the public body will make of the personal information.

The *legal authority* for collection may be an enactment of Alberta or Canada that expressly authorizes collection of the personal information, or **section 32(c)** of the *FOIP Act*, which authorizes collection of personal information that is directly related to and necessary for an operating program of a public body.

If a public body relies on **section 32(c)** of the *FOIP Act*, it is important to provide the authority for the program. This is to increase people's awareness of the actual authority by which public bodies collect personal information. The program itself may be authorized by an Alberta or federal Act or a regulation under an Act, or a by-law or legal resolution of a public body establishing a program that falls within its mandate under an Act.

Identifying someone to answer the individual's questions about the collection is intended to provide the individual with a knowledgeable source of information. The person cited should be familiar with the program, and be able to explain why the personal information is being collected and how it will be used, retained, and disclosed to other organizations.

Public bodies should undertake regular review of their collection instruments to determine which ones require the inclusion of collection notices.

Collection notices should be included on all forms used to collect personal information directly. This should be done in conjunction with the review discussed in section 7.2 of this chapter and any review of information practices, as discussed in Chapter 9 of this publication.

Exception to Notification

Section 33(3) provides that the requirement of **section 33(1) and (2)** may be set aside if, in the opinion of the head of the public body, compliance with these provisions could reasonably be expected to result in the collection of inaccurate information.

This provision recognizes that in certain limited circumstances, such as the conduct of some surveys seeking opinions and in some psychological testing, there may be difficulty in getting accurate information if individuals are informed in advance of the reasons for the collection.

An example of a situation where a public body might not reasonably expect to obtain accurate information directly from the individual concerned would be the collection of information about participants in a literacy program who cannot read, write or understand English.

Inaccurate information is wrong, incomplete or misleading information, or information which does not reflect the truth. In the case of some surveys, notifying individuals of the purpose of the survey would lead to responses that would distort the results.

This provision is intended to be used in limited circumstances and public bodies should maintain documentation of when the provision has been used and the reasons for using it.

7.4 ACCURACY AND RETENTION

Section 34 of the *Act* provides that, if a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must:

- make every reasonable effort to ensure that the information is accurate and complete; and
- retain the personal information for at least one year after using it so that the individual has an opportunity to obtain access to it.

Retention may be for a shorter time period under certain conditions discussed below in relation to **section 34(b)** of the *Act*.

A decision that directly affects the individual is one that has an immediate impact on the person's life. The meaning of the term is interpreted broadly and includes decision-making processes that are internal to a public body and those which involve a more direct relationship with the public.

Examples of decisions that directly affect an individual include a determination as to whether or not someone is entitled to income assistance or a student loan, a decision on hiring an individual or on admission to a course or program, and a determination regarding eligibility for health services or library services.

This requirement does not extend to situations where no decision, adverse or otherwise, will be or has been made about an individual. Examples include raw survey data where personal information is collected but the results are rendered anonymous, telephone messages, and unsolicited resumes that are never considered in relation to a position.

Accuracy

Section 34(a) requires the public body to make every reasonable effort to ensure that personal information is accurate and complete.

A public body makes *every reasonable effort* when it is thorough and comprehensive in identifying practicable means to assure that personal information in its custody or under its control is accurate and complete.

Generally, if a public body collects personal information directly, it is likely to meet the requirement of making every reasonable effort. This is especially so if the individual has signed a statement indicating that the information is complete and accurate.

Compliance with this provision involves careful verification of any personal information crucial to an application, transaction or action at the time the information is provided. A public body should also have systematic processes for updating personal information when it is used on a regular or continuous basis. This can be done using information provided by the individual or cross-referencing other related files providing basic identifying data.

Other checks of accuracy might consist in having periodic audits of files with accuracy and completeness as one of the criteria tested; ensuring limited access to information for the purpose of making corrections; and establishing cross-referencing and verification checks within the software of automated systems that identify anomalies in data.

The accuracy requirement of **section 34(a)** of the *Act* requires public bodies to have some type of verification procedure, but this is also good business practice for programs that use large personal information systems for delivery of programs or services.

Privacy requirements should be integrated into normal information and systems operations for the program as a whole.

The Commissioner has also said that ensuring accuracy includes making certain that hand-written information used to make decisions, such as clinical notes, is legible (see *IPC Order 98-002*).

Retention

Section 34(b) requires public bodies to retain personal information for at least one year after using it to make a decision that affects an individual, so that the individual has a reasonable opportunity to obtain access to it.

This does not include personal information in transitory records if the information is transferred to a different format. This may be the case with records such as counselling notes or notes of an interview panel member that are consolidated into a final document, if it is the policy of the public body to treat these notes as transitory records. (See Chapter 8.6 of this publication for further discussion of transitory records.)

This provision is intended to permit individuals to review and, if necessary, to request correction of information about them that has been used by public bodies before disposition of that information takes place.

Section 34(b) overrides all records retention and disposition schedules by establishing a retention period of one year after use for personal information used in administrative decision-making.

An exception to this requirement is allowed when a public body and the individual the information is about both agree in writing to a shorter retention period. In the case of government departments and agencies subject to the Records Management Regulation, a decision not to retain the personal information requires additional approval from the Alberta Records Management Committee.

This exception might be used, for example, to permit destruction of a person's application for counselling or addiction treatment when the applicant withdraws the application and does not seek the treatment.

Retain means to maintain custody or control of the personal information. The requirement to retain information means that the information cannot be destroyed, but it could be moved to a records storage facility such as the Alberta Records Centre.

Section 34(b) does not prevent public bodies from storing personal information in another location if the public body can retrieve the personal information in response to a request for access to it.

Public bodies may keep personal information longer than one year, depending on their operational needs and on legal requirements. To help ensure that out-of-date and incomplete personal information is not incorrectly used in a decision affecting an individual, personal information should be scheduled for retention and disposition in accordance with the appropriate authorities for the management of recorded information. **For provincial public bodies, this must be done in accordance with policies and procedures established under the *Government Organization Act* and the Records Management Regulation. For local public bodies it should be done in accordance with local records management policies and retention and disposition schedules.**

If a public body receives a request for access to personal information during the one-year retention period, it must keep that personal information with the request file for a further year after the last action is taken in regard to the request.

If the Information and Privacy Commissioner conducts a review of the response to an access request that contains personal information, the information must be retained for a year from the date that the Commissioner makes a decision.

It is not necessary to retain personal information when no decision will be or has been made about individuals.

7.5 CORRECTION OF PERSONAL INFORMATION

Section 35(1) provides that an individual may request that a public body correct personal information about that individual that is in the public body's custody or control if the individual believes that it contains an error or omission.

This provision applies only to the applicant's own personal information. The public body may either correct the information, by changing it or adding new information, or may refuse to correct the information, subject to other provisions discussed below.

An *error* is mistaken or wrong information or information that does not reflect the true state of affairs. An *omission* is information that is incomplete or missing or that has been overlooked.

A public body has *custody* of a record when the record is in the possession of the public body and the public body has a right to deal with the record and some responsibility for its care.

A record is under the *control* of a public body when the public body has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition.

See Chapter 1 of this publication for a detailed discussion of custody and control.

Information is personal information if it meets the definition of personal information in **section 1(1)(n)** of the *Act*, regardless of how a public body comes to have that personal information (see *IPC Order 98-001*).

When considering requests for correction of personal information, it is important to distinguish between the two types of information addressed by **section 35**:

- *factual information* about the applicant, such as age, date of birth, income information or qualifications (**section 35(1)**); and
- *opinions* about the applicant, such as subjective assessments or evaluations of an individual's condition, abilities or performance (**section 35(1.1)**).

The applicant must provide proof in support of the request for correction of factual information. The proof should be of the same nature and at least the same quality as the personal information required when the original collection took place. Examples of documents that might be required to prove facts include a birth or baptismal certificate to prove age, or a notice of assessment from Revenue Canada to prove income.

A public body *must not* correct an opinion (section 35(1.1)) including a professional or expert opinion. This provision recognizes that the significance of an opinion may be that it reflects another person's view at the time it was offered, and it may be important to have a record of that view at a later date. The *Act* allows an individual to have his or her views about that opinion added to the record for other readers to consider.

Although a public body cannot correct an opinion, it may, in some circumstances, seek or accept another opinion about the applicant and reconsider any decision based on the original opinion.

How a Request is Made

In many cases, an individual will ask for personal information to be corrected and supply proof of correction without doing this in a formal way. Public bodies can, and most often will, make corrections without a request under the *Act* if this is practical and expedites public business.

The formal process for an individual to determine whether or not an error or omission exists in a record is for that individual or a representative to request and review the personal information in accordance with the procedures set out in **Part 1** of the *Act*.

Where an error or omission exists, in the opinion of the applicant, a request for correction can be made to the public body in the form of a letter or on a **Request to Correct Personal Information Form**, a sample of which is included in Appendix 6 of this publication.

Requests for correction are subject to the same rules as requests for access under the *Act*. This includes time limits. It also includes a duty on the part of the public body to fully understand and seek clarification of a correction request (see *IPC Order 98-010*).

The Commissioner has the power to review the actions of a public body with respect to requests for correction of personal information.

When a Correction is Made

When a public body accepts a request for correction of an error, all records containing the personal information are corrected. This includes records in all information systems – paper, electronic and microform. Similarly, when a public body agrees to add omitted information, all systems must be updated. The record should be annotated with the date of the correction. A linking mechanism, as described below, may have to be employed when personal information is stored on a medium such as microform, which may be more difficult to update.

To *annotate* personal information is to note the requested correction on the record, close to the information under challenge by the applicant. An annotation should be signed and dated. When designing electronic forms and databases, care should be given to allow for annotations. (For a discussion of annotation, see *IPC Order 97-020.*)

To *link* a record means to attach, join or connect the record to the requested correction. This may consist of a letter or statement from the applicant, or a copy of the **Request to Correct Personal Information Form**.

When a public body makes an annotation or linkage, it must ensure that the new information is stored and retrieved with the original information whenever the information in question is used for an administrative purpose directly affecting the individual involved. As well, annotations must be made available to the individual should he or she request access to his or her personal information (see *IPC Order 97-020*).

When a Correction is Refused

Section 35(2) provides that, when a correction is refused or cannot be made, the public body must annotate or link the personal information with that part of the requested correction which is relevant and material to the record in question.

Relevant and material means that there is a direct connection between the correction requested and the use that has been or may be made of the personal information and that the correction is substantive. The correction should be both pertinent to the subject matter and significant in its content.

A public body may refuse or be unable to make a correction that an applicant requests. This may be because the information is not personal information, the applicant has not submitted adequate proof in support of the requested correction, or the information consists of an opinion rather than fact (see *IPC Order 98-010*).

In the case of factual information, when the public body is not satisfied with the proof presented, it does not change the information but rather annotates it or links the presented information to the original information.

In the case of an opinion, a public body may describe the information in dispute and place this description, along with a statement that the applicant does not agree with the opinion or interpretation, on the record. If practicable, the applicant's request for correction may be attached (see *IPC Order 97-020).*

Only that part of the requested correction which is relevant to the record being annotated or to which the link is being made is noted. Public bodies are under no obligation to place the applicant's entire request on the record if it contains material that is not germane to the use made of the record.

A model **Annotation Form** is provided in Appendix 6 of this publication. A public body may use this form to set out an annotation relating to a correction that was requested but not made. This form clearly indicates to users that the information has been linked to a correction request and not corrected. It is filed with, or linked to, the information for which a correction was sought.

A copy of this form or equivalent documentation must be sent to the individual requesting a correction at the time that he or she is informed that the correction is not being made (see Model Letter S in Appendix 3 of this publication). Any further information supplied by the individual after he or she received this notice must be filed with the Annotation Form.

If the **Annotation Form** or the **Request for Correction Form** cannot be physically attached to the record, a flag may be placed in the file or system containing the personal information in dispute. This will refer a user to a separate file, containing the actual disputed personal information, and indicating that a request for correction or addition of information was made but not granted.

When a public body makes an annotation or linkage, it must ensure that the new information is stored with the original information and will be retrieved whenever the information in question is used for an administrative purpose directly affecting the individual involved. As well, annotations must be made available to the individual should he or she request access to his or her personal information.

Notification of Other Public Bodies and Third Parties

Section 35(3) obliges public bodies to inform other public bodies, groups of persons, persons, or organizations that have received an applicant's personal information from the public body that the applicant has requested a correction or annotation. Notification is required if the personal information has been shared in the year prior to the request for correction.

The notification process ensures that other parties have accurate and complete information for their own decision-making processes.

Section 35(3.1) provides that such notification is not necessary if:

- the correction, annotation or linkage is not material; and
- the individual who requested the correction is advised and agrees in writing that notification is not necessary.

This allows public bodies to dispense with third party or public body notification if the correction requested is not required for their decision-making. **To ensure that the applicant is advised and agrees with this assessment, consent in writing is required in each instance.**

Section 35(4) provides that other public bodies, once notified, must make any correction, annotation or linkage to the relevant personal information disclosed to them and which is in their custody or under their control. This helps ensure that all personal information shared between public bodies is accurate and complete.

Time Limits

Section 35(5) provides that a public body must, within 30 days of receiving the request, give written notice to the individual that either the correction has been made or an annotation or linkage has been made. It is good practice to ensure that other public bodies or third parties are also notified within the 30-day time period.

A public body may extend the time limit to deal with a request for correction for up to 30 days or, with the permission of the Information and Privacy Commissioner, for a longer period.

Section 13 of the *Act* governs these extensions and the most likely to apply in correction situations are:

- the applicant does not give enough detail to enable the public body to identify a requested record (**section 13(1)(a)**); and
- a large number of records is requested or must be searched and responding within the time limit would unreasonably interfere with the operations of the public body (**section 13(1)(b)**).

Model letters R, S and **T** in Appendix 3 of this publication deal with the correction process. Guidance on making corrections and annotations, as well as copies of the **Request to Correct Personal Information Form** and the **Annotation Form** are included in Appendix 6 of this publication.

Transfer of Requests for Correction

Section 35.1 provides authority for a public body to transfer a request for correction of personal information to another public body. This can occur when:

- the other public body originally collected the personal information; or
- the other public body created the record containing the personal information.

This provision ensures that the public body that originally collected or compiled the information deals with a request for the correction of personal information. It can also ensure that all public bodies in receipt of that information are properly notified of the correction. **Section 35.1** mirrors the provisions for transfer of access to information requests.

If a request is transferred under this section, the public body transferring the request must notify the applicant of the transfer as soon as possible. The public body receiving the transferred request has 30 days from the date of the transfer to respond to the request, and can extend this time limit as outlined above.

7.6 PROTECTION OF PERSONAL INFORMATION

Section 36 of the *Act* requires a public body to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

Making *reasonable security arrangements* means approving and implementing a security policy for use within a public body.

The policy should address physical, administrative and information technology security. It should be geared to a risk and threat analysis of the information in the custody or under the control of a public body.

The policy should assign accountability for carrying out security measures and cover responsibilities and arrangements for protecting personal information. It should also establish requirements for training personnel about appropriate security standards and the application of these to support privacy protection.

The security measures for personal information should be based both on the size of the public body and the results of the risk and threat analysis.

Small public bodies with little personal information in electronic form should concentrate on physical security measures. Larger organizations with sensitive personal information in a variety of forms and media will have to take a wider range of security measures.

The sensitivity of personal information varies widely. For example, some types of medical and financial information have high sensitivity and there is a greater possibility of damage to an individual if they are accidentally disclosed, are stolen or find their way into unauthorized hands in some other way.

Such information requires stringent protection measures, which may include physical access control zones, locked rooms, locked filing cabinets, and personnel reliability checks. Information technology systems may require computer access control codes, automatic tracking of use and telecommunications security devices.

As information systems are implemented that involve more sophisticated technology, security measures should be commensurate with this. For example, data encryption, public key infrastructures and other privacy-enhancing technologies may be employed.

More routine case files which deal with relatively few elements of personal information, and where the risk of compromise or unauthorized access is low, will require lower grade security measures. These may include locked cabinets, a controlled area that is locked at night, and computers that are kept behind service counters and are accessed through restricted authorization codes.

Public bodies should analyze the types of personal information in their custody or under their control, the varying levels of sensitivity for each type of personal information and the risks and threats that apply to them.

They must take the necessary steps, over time and within available resources, to implement security policies, requirements and procedures relating to the protection of personal information that is sensitive and at risk.

Section 36 also applies to personal information disclosed to or collected or compiled by contractors. Public bodies should ensure that their contracts contain adequate security clauses.

The basic features of a security policy that recognizes privacy protection requirements are set out in Chapter 9 of this publication.

Unauthorized access refers to situations where employees have access to personal information that they do not need to see or handle in the course of their employment. It also refers to situations where members of the public gain access to personal information about other individuals to which they have no right. This may happen through an accidental disclosure or through surreptitious means. Public bodies should have policies in place to verify the identity of those requesting personal information (see *IPC Investigation Report 98-003*).

Unauthorized collection occurs when personal information is gathered, acquired, received or obtained by any means for purposes that are not allowed under **section 32** of the *Act*. See the discussion of collection in section 7.2 of this chapter. This includes collection through interviews, questionnaires, surveys, polls, audio tapes, video tapes, electronic means, forms, telephone calls, and letters.

It is the responsibility of the public body to ensure that personal information is collected in accordance with **sections 32** and **33** of the *Act*.

Unauthorized use is the use of information for a purpose that is not permitted under **section 37** of the *Act*. The requirements of this provision are discussed in section 7.7 of this chapter.

The public body is responsible for ensuring that uses of personal information are authorized under **section 37**.

Unauthorized disclosure refers to the act of revealing, showing, providing copies, selling, giving, or relating the content of personal information in ways that are not permitted under **section 38** of the *Act*. It includes oral disclosure (see *IPC Investigation Report 98-003*). The requirements of this provision are discussed in section 7.8 of this chapter.

The public body is responsible for ensuring that all disclosures of personal information are authorized under **section 38**.

Unauthorized destruction of personal information means the destruction of records containing personal information in ways that are not permitted under **section 3(e)** of the *Act*.

Personal information may be at risk of unauthorized disclosure during the disposition process. For example, files containing personal information have been found scattered in the rear of public buildings and left on the hard disks of computers disposed of by a public body.

Destruction of personal information to prevent access by the individuals to whom it refers is unauthorized disposal which is an offence under section 86(1)(e) of the *Act*.

Public bodies should ensure that procedures and practices for the disposal of personal information form part of their corporate policy on the management of recorded information. This is discussed in more detail in Chapter 8 of this publication.

Most provincial public bodies are subject to the records management policies and procedures deriving from the *Government Organization Act* and the Records Management Regulation.

For other public bodies, disposal of personal information should occur only in accordance with policies and procedures approved by the governing body. Generally, these will be included in the by-law, resolution or other legal instrument that approves the storage, transfer or destruction of public body's records (**section 3(e)**).

Authorized disposal of personal information may occur through:

- transfer of the record to the custody of the Provincial Archives of Alberta or the archives of a public body;
- physical destruction of the record containing personal information in such a way that it cannot be retrieved or reconstructed; or
- alienation of the record as a result of a privatization arrangement or the transfer of service delivery to a body not subject to the Records Management Regulation. A public body that is subject to the Records Management Regulation must have a Records Alienation Schedule approved by the Alberta Records Management Committee to authorize the transfer of records to a private-sector organization.

Standards for the transfer and destruction of records of provincial public bodies are found in the publication *Records Scheduling and Disposition in the Government of Alberta*, produced by Alberta Innovation and Science.

Examples of unauthorized destruction would be the shredding of information with no authority to do so, the simple discarding of personal information in a garbage container or recycle bin, or the sale of a computer without ensuring that personal information is completely and permanently removed from the hard disk.

Public bodies should document the transfer of records containing personal information to the Provincial Archives or other archives and the destruction of records containing personal information. This does not apply to transitory records.

For provincial public bodies, written notice of any inadvertent destruction of records must be provided to the Alberta Records Management Committee.

Public bodies are responsible for ensuring that personal information is protected during the time it is in storage and in the process of being transferred to archives or destroyed.

7.7 USE OF PERSONAL INFORMATION

Section 37 of the *Act* lists the *only* circumstances under which a public body may use personal information. These are:

- for the purpose for which the information was collected or compiled or for a use consistent with that purpose (**section 37(1)(a)**);
- if the individual the information is about has identified the information and consented, in the prescribed manner, to the use (**section 37(1)(b)**);
- for a purpose for which that information may be disclosed under **sections 38, 40** or **41** (**section 37(1)(c)**); or
- if the information is in alumni records, for the purpose of a post-secondary educational body's own fund-raising activities (**section 37(2)**).

Use of personal information means employing it to accomplish the public body's purposes, for example, to administer a program or activity, to provide a service or to determine eligibility for a benefit.

In **section 37(1)(a)**, the *purpose* is the object to be attained by the collection of the information or the thing intended to be done with it. It includes the administration of a particular program, the delivery of a service and other directly related activities.

The *purpose* must conform to **section 32** of the *Act*, which limits the purposes for which information may be collected. This is discussed in section 7.2 of this chapter.

Collection must be authorized by an Act or regulation, or it must be for the purpose of law enforcement as defined in **section 1(1)(h)**, or it must be necessary for an operating program or activity of the public body.

The purpose of collection is described in the collection statement provided to the individual when the information is collected directly. When the information is not collected directly, or when it is compiled from several sources, the purpose should be stated in the written policy or procedure dealing with the program.

Information may be *collected or compiled.*

To *compile* information is to draw information from several sources and create a new set of information. It can also mean the creation, calculation, linkage, interpolation or extrapolation of data to produce new information.

A public body may make use of personal information it has gathered, created or manipulated for the specific purposes for which it is permitted to obtain it.

Section 37(1)(a) also permits uses *consistent* with the original purpose.

Consistent use is defined in **section 39** of the *Act* as a use that is directly related to the original purpose of collection and that is necessary for performing the statutory duties of the public body.

Section 7.9 of this chapter deals more thoroughly with the concept of consistent uses.

Public bodies must keep a complete, current and accurate record of all uses of personal information held in personal information banks (**section 82(3)**).

Consent of the Individual

Section 37(1)(b) permits use of personal information if the individual the information is about has identified the information and has consented, in the prescribed manner, to its use.

An individual has *identified* the information means that:

- the individual is aware of the specific information that the public body intends to use;
- the public body has informed the individual about the purpose for which the personal information will be used; and
- the public body has informed the individual about any consequences of agreeing or refusing to consent to the use.

Has consented *in the prescribed manner* means that the public body has followed the procedures for obtaining consent set out in **section 6** of the FOIP Regulation.

This states that consent:

- must be in writing; and
- must specify to whom the personal information may be disclosed and how the personal information may be used beyond the original purpose for which the personal information was collected or compiled.

Where appropriate, a form or other instrument requesting consent should:

- **indicate the original purpose of the collection, as well as the additional purpose for which the information is to be used and for which consent is being provided;**

- **indicate that consent is voluntary;**
- **indicate that consent may be revoked at any time;**
- **to the extent possible, identify any consequences that may result from refusal to consent; and**
- **indicate the period of time during which the consent remains valid.**

A public body may seek consent for a new use of personal information when updating personal information or when collection has to be repeated. The collection statement required under **section 33(2)** should be revised, and use of personal information collected from individuals after that time will be in accordance with the revised purpose.

The different use would be noted at the time of collection, usually on the collection instrument or through pop-up screens for electronic collections. The notification would include the purpose of the collection, a statement that consent is voluntary, identification of any consequences which may result from refusal of consent, and the period of time for which consent will remain valid. Space or opportunity should be provided for the individual to clearly indicate whether or not he or she gives consent to the use.

Approval of a different use by the individual concerned serves as an indication that the person knows the consequences of the use of his or her personal information and has been provided with enough facts to make an informed decision about whether or not to agree to the use.

When the person concerned has not indicated whether or not consent is given to a different use of personal information, public bodies cannot assume the individual has consented.

The absence of consent must be interpreted as the absence of authorization.

Public bodies cannot penalize individuals for refusing to give consent for use for an *additional* purpose by denying them any benefit or service provided through the original collection. Individuals may, however, find they are denied a benefit or service that might have been made available if the individual had consented to use of his or her personal information for that different purpose.

Section 7.13 of this chapter deals with those classes of persons who may act for minors, incompetent persons, and other individuals in giving or withholding consent.

A Purpose for Which Information may be Disclosed to a Public Body under Sections 38, 40 or 41

Section 37(1)(c) provides that a public body may use personal information that is disclosed to it by another public body under **sections 38, 40** or **41** of the *Act*.

Without this provision, a public body would be unable to use personal information disclosed to it in an authorized way. This provision assists in eliminating duplicate collections of personal information by permitting public bodies to use personal information that can be disclosed by another public body under **section 38**.

It also allows a public body to use personal information disclosed to it for research purposes by another public body under **section 40** or by the Provincial Archives or the archives of another public body under **section 41.**

Alumni Records of a Post-Secondary Educational Body

Section 37(2) provides that a post-secondary institution may use personal information in its alumni records for the purpose of its own fund-raising.

This provision recognizes that colleges and universities have historically used alumni records for fund-raising purposes. Post-secondary educational bodies should have procedures in place to inform new alumni of this use at the time of graduation. They should not rely on this provision, which was added to the *Act* in May 1999, to use the personal information of individuals who become alumni *after* 1999 for their fund-raising activities.

The use of this personal information is qualified by **section 37(3).** This requires the public body to discontinue using an individual's personal information for fund-raising purposes when requested to do so by that individual.

Post-secondary educational bodies should take reasonable steps to inform their alumni of this provision. This might consist of placing a notice in a prominent place in the institution's alumni newsletter to give individuals a chance to request cessation of the activity, or providing alumni with an opportunity to request cessation of the activity when mailing lists are updated, or mailing a notice to all alumni. For more information on this topic, see *FOIP Bulletin No. 5, Fund-Raising.*

Constraint on Use of Personal Information

Section 37(4) sets some limits on the extent to which a public body can use the personal information in its custody or control.

A public body can use information only to the extent necessary to carry out its purpose in a reasonable manner.

For example, employees in a particular program area who have access to personal information in an electronic database should be provided with access to only those data elements they require to do their job, not to the whole database.

In a reasonable manner means in such a way that a public body is not required to implement overly restrictive procedures on use of personal information when the information is not of a sensitive nature or when disclosure would not be harmful to personal privacy. Severing of information or restricted access to electronic data would be considered on a program-by-program basis.

This statement mirrors the statement covering disclosure of personal information in **section 38(2).**

It ensures that public bodies to which personal information is disclosed are subject to the same rules as the public body disclosing the information. It is intended to limit disclosure to the minimum amount of information needed to accomplish the purpose of disclosure, and to limit use to the minimum necessary to achieve the purpose of the public body using the information.

7.8 DISCLOSURE OF PERSONAL INFORMATION

Section 38 of the *Act* lists the *only* circumstances under which public bodies may disclose personal information. It provides for a response to an access request under **Part 1**, or disclosure in the absence of a formal access request.

The word *only* indicates that disclosures of personal information are limited to the specific circumstances outlined in **section 38**. If **section 38** does not provide authority for a disclosure, the public body cannot disclose the information.

Section 38 *enables* disclosure; it *does not require* disclosure. This is indicated by the word *may* in the introduction to the section. Public bodies should look at the circumstances surrounding each request when deciding whether to disclose personal information. They should also disclose only the information pertinent to the request.

Section 38(2) states that a public body may disclose personal information only to the extent necessary to enable it to carry out the purposes described in immediately preceding subsections. These purposes are described in the following pages. Disclosure has to be carried out in a reasonable manner (see section 7.7 of this chapter).

Public bodies should be careful to disclose only limited amounts of personal information. They have a responsibility in most cases to clarify and understand the reasons for the request for disclosure. Disclosures should be made in a way that helps the requester and is cost-effective for the public body. This may mean that not all disclosures are in writing, or that, when a working relationship has been established, all the proofs required are not asked for each time a request is made.

Disclose means to release, transmit, reveal, expose, show, provide copies of, tell the contents of, or give personal information by any means to someone. It includes oral transmission of information by telephone or in person; provision of personal information on paper, by facsimile copy or in another format; and electronic transmission through electronic mail, data transfer or the Internet. The disclosure may be made:

- to the person whose information it is, either in response to a routine request for information or in response to a FOIP request;
- to an individual's personal representative who is entitled to exercise the rights of that individual under **section 79** of the *Act*;
- to any other person in response to a FOIP request, as a release in the public interest, when the disclosure would not be an unreasonable invasion of privacy, or when **section 38** of the *Act* specifically allows the disclosure; or
- to other public bodies, to legislative, legal and judicial officers, to other levels of government, or to non-government organizations. These disclosures may take place to support the activities of either the public body disclosing the information or the party to which it is disclosed.

Public bodies should keep a record of any disclosures of personal information made under **section 38**. This may consist of a note on a file or a flag in an electronic system that refers to a paper record or another data file. **A record of disclosures is needed to enable a public body to comply with its obligation under section 35(3) to inform anyone to whom it has disclosed personal information of any correction to that information.**

Such records of disclosure should include:

- the name of the individual whose personal information is requested;
- the nature of the requested information and the purposes for which it will be used;
- the authority for the request;
- the title, business address and business telephone number of the contact person in the requesting public body or agency; and
- the name and signature of the officer or employee of the public body who authorizes the use or disclosure.

Public bodies must have appropriate administrative controls in place to ensure against the disclosure of personal information to anyone who is not permitted access to the information under the provisions of the *FOIP Act*.

Public bodies should regularly review their disclosure policies and practices to ensure that they meet the requirements of the *Act*. Where it is found that disclosures are not authorized, practices should be altered to meet legal requirements or discontinued.

A review may be carried out in conjunction with a review of information practices and systems discussed in Chapter 9 of this publication.

Section 38 does not prevent the routine disclosure of an individual's personal information to that individual if the public body has adopted a policy of disclosing that category of personal information. In these circumstances, the public body will provide the personal information without a FOIP request.

Public bodies must keep a current, accurate and complete record of the purposes for which personal information held in any personal information banks may be disclosed (**section 82(3)**).

In the following pages, each permitted disclosure is outlined and discussed.

***In accordance with Part 1 of the Act* (section 38(1)(a)):** This provision permits disclosure to respond to access requests and to comply with the public interest provisions of the *Act*. A disclosure may take place when:

- an applicant has requested access to his or her own personal information, subject to the exceptions in **sections 15 to 28** and the paramountcy provision in **section 5**;
- an applicant has requested access to records containing personal information about another individual and disclosure of the personal information does not constitute an unreasonable invasion of the privacy of the other individual under **section 16**, subject to other exceptions and to third party notification requirements; or
- **section 31** applies.

***Disclosure would not be an unreasonable invasion of a third party's privacy under section 16* (section 38(1)(a.1)):** This provision permits disclosure when it is clear that the personal information would not be excepted under **section 16**. It is intended to permit disclosure of personal information described in **section 16(2)** without the necessity of a FOIP request.

This provision gives public bodies more flexibility in responding to requests for personal information that clearly would be provided if a FOIP request were made. It allows for a more helpful and timelier response to such requests.

When another provision of **section 38** permits disclosure, the disclosure should be made under that provision. Examples are: disclosure with the consent of the individual, disclosure required or authorized by an Act of Alberta or Canada, and disclosure for research purposes.

In some circumstances, public bodies will be able to establish policies and practices for routine disclosure in response to requests for particular classes of personal information. In establishing such policies, public bodies should determine whether any of the other exceptions outlined in **Part 1** of the *Act* might apply to the information.

Examples of classes of personal information for which a policy might be appropriate include:

- information about employee classification, salary range, employment responsibilities and discretionary benefits (**section 16(2)(e)**);
- financial and other details of a contract to supply goods or services (**section 16(2)(f)**);
- information regarding permits or licences relating to commercial or professional activities or real property (**section 16(2)(g)**);
- details of discretionary benefits of a financial nature (**section 16(2)(h)**); and
- personal information about an individual who has been dead for 25 years or more (**section 16(2)(i)**).

Public bodies may charge a fee for such information.

For more information on **section 16(2),** see Chapter 4.4 of this publication.

Section 16(2)(j) deals with a range of disclosures that can be made if disclosure is not contrary to the public interest. Individuals have the right to request that the information outlined in this provision not be disclosed. For this reason, requests for personal information that falls within the scope of **section 16(2)(j)** need to be considered on a case-by-case basis. A public body may take into consideration who is making the request, and why, in deciding whether to disclose the information.

If an individual has requested that the information not be disclosed, it cannot be disclosed under **section 38** unless another provision in the section allows it and the public body decides to disclose the information against the wishes of the individual.

If disclosing the information could interfere with law enforcement or could reasonably be expected to affect someone's health or safety, it should not be disclosed.

For more information on situations when disclosure might be made, see Chapter 4.4 of this publication and *FOIP Bulletin No. 4, Disclosure of Personal Information – Section 16(2)(j)*. The examples that follow are illustrative only.

***Enrolment in a school, or in a program of a post-secondary educational body*:** This provision allows confirmation of the fact that an individual is, or was, enrolled in a particular school or a particular program of a post-secondary body.

Examples of permitted disclosures include:

- providing parents with a list of students in a music program or other program that requires collaborative effort outside the school or post-secondary body;
- providing a list of past students in a school or post-secondary program to facilitate a reunion or other social event;
- providing a list of the grade 12 graduating class to graduation event organizers or the local news media;
- publishing photographs of students in a college calendar; and
- posting or publishing class photographs.

***Admission to a health care facility*:** This provision allows confirmation of the fact that an individual is currently in a hospital or other health care facility. It also allows confirmation of current residence in a long-term care facility. It does not apply once a person has left the health care facility or institution, at which time the public body may only confirm than an individual is not currently a patient or resident. Nor does it allow disclosure of any information about the individual's treatment. **Public bodies should be aware of other health legislation that may restrict disclosure under this provision.**

Examples of disclosures that might be permitted under this provision include:

- confirming that a friend or relative is currently a patient in a hospital;
- confirming that an individual is currently in the emergency department of a hospital;
- providing a list of current hospital patients to the clergy or a pastoral care team; and
- providing a list of residents in a nursing home to a disabled adult transportation service.

***Attendance at or participation in a public event or public activity*:** This provision allows disclosure of the fact that a person attended or participated in a public event organized by a public body. A record of attendance or participation would have to exist to allow disclosure to take place.

A public event is something that is noteworthy, supervised or organized in some way and is intended to be accessible to the public. It includes events where admission is by ticket and events where the media are present together with other members of the public.

Examples of permitted disclosures under this provision include:

- providing a list of attendees at an open house or fund-raising event;
- providing a list of participants on a field trip to the person receiving them at the destination;
- providing names and photographs of players at a sporting event;
- providing the names of students participating in a science fair or art exhibition; and
- announcing the names of individuals in the graduating class for a specific year.

***Receipt of an honour or award granted by or through a public body*:** This provision allows disclosure of the fact that a person has received an honour or award, including disclosure of a photographic record of the ceremony. This provision *does not* allow disclosure of offers of or qualification for an honour or award if it was not presented, or of an offer of an award that an individual has declined. Nor does it allow disclosure of the names of persons considered for an award but not granted one. Awards and honours that may be disclosed include those granted by the public body on behalf of a private corporation or individual.

Examples of personal information that might be disclosed under this provision include information relating to:

- graduation certificates or awards;
- degrees, including honorary degrees;
- scholarships, prizes or bursaries;
- inclusion in honour rolls;
- merit or recognition awards;
- long-service and retirement awards; and
- appointments to honorary offices.

***Original and consistent uses* (section 38(1)(b)):** This provision permits disclosure for the purpose for which the information was collected or compiled or for a purpose consistent with that purpose.

The *purpose* for which personal information was collected or compiled means the object to be attained or the thing intended to be done. Generally, that is the administration of a program or the provision of a service. Such purposes must conform to **section 32** of the *Act*, which limits the purposes for which information may be collected. This is discussed in section 7.2 of this chapter.

Personal information is *compiled* when it is assembled from several sources or generated, calculated, extrapolated, interpolated, linked, deduced, or otherwise created. The word implies collection from more than a single source and not directly from an individual.

A *consistent use* is one that has a direct and reasonable connection to the original use and that is necessary for performing the statutory duties of, or for operating an authorized program of, the public body (**section 39**). A disclosure is therefore permissible if it is a logical extension of the original use.

Examples of consistent uses include:

- providing a list of participants in a program to another part of a public body for evaluation of the program;
- using the assessment roll to confirm property ownership when needed for other municipal purposes; and

- disclosing information to another public body which is carrying out a part of the program for which the personal information was originally collected.

A more detailed explanation of *consistent use* is provided in section 7.9 of this chapter.

Consent to disclosure **(section 38(1)(c)):** This provision permits disclosure of an individual's personal information when the individual has identified the information and consented, in the manner prescribed in **section 6** of the FOIP Regulation, to the disclosure.

The individual has *identified* the information means that the public body has informed the individual about:

- the specific information that the public body intends to disclose;
- the purpose for which the personal information will be disclosed; and
- any consequences of agreeing or refusing to consent to the disclosure.

Consent for a disclosure should be sought as early as possible after the need has been identified. Ideally, it should be sought at the time the information is collected. In such cases, the request for consent to disclose is added to the collection instrument, indicating:

- to what public body, group or organization the information may be disclosed;
- that consent to disclosure is voluntary, noting any consequences that may result from refusing to consent to the disclosure; and
- the period for which the consent will remain valid.

The same procedure for obtaining and recording consent to disclosure may be used when personal information is collected for an administrative process that will be periodic and ongoing.

In the case of electronic collection, pop-up screens can be used to provide notification to the individual, provide the requisite explanations and enable consent or refusal. In all instances, space or opportunity should be provided for the individual to clearly indicate whether consent to the disclosure is given.

Section 6 of the FOIP Regulation states that consent under **section 38(1)(c)**:

- must be in writing; and
- must specify to whom the personal information may be disclosed and how the personal information may be used beyond the original purpose for which the personal information was collected or compiled.

The absence of consent is interpreted as the absence of authorization. When the person concerned has not indicated any consent to disclosure of personal information, and no other provision exists to permit disclosure, public bodies cannot disclose information.

A public body must not penalize an individual for refusing to consent to a disclosure of personal information for a purpose other than the purpose for which the personal information was collected. A public body must not deny the individual the benefit or service for which the personal information was originally collected.

Consent may be given by a representative acting on behalf of an individual in accordance with the conditions set out in **section 79(1)**. These conditions are discussed in detail in section 7.13 of this chapter.

Examples of consent to disclosure include: agreement to have references provided in support of job applications; agreement to provide information to Revenue Canada in order to obtain income verification from that source; consent to disclosure in response to third party notice under **section 29** and agreement to the use of photographs for promotional purposes.

***Disclosure to comply with an enactment of Alberta or Canada or with a treaty, agreement or arrangement* (section 38(1)(d)):** This provision permits disclosure of personal information to comply with an Act of Alberta or Canada, a regulation made under such an Act, or with a treaty, arrangement or agreement made under either an Act or a regulation. It does not apply to the legislation of other provinces, territories or foreign states.

Public bodies should prepare a list of all agreements, arrangements and treaties, as applicable, under which they disclose personal information. Public bodies should include such information in the relevant personal information bank descriptions contained in the directory of personal information banks which the *Act* requires to be maintained for the information of the public (**section 82(3)**).

Disclosure to *comply with an enactment of Alberta or Canada* means disclosure of personal information as *required* by either provincial or federal legislation. The enactment must impose an obligation to disclose the personal information.

Disclosure to *comply with a treaty, arrangement, or agreement* made under an enactment of Alberta or Canada means disclosure of personal information as *required* by the treaty, arrangement or agreement. The enactment must provide authority for the provision in the treaty, arrangement or agreement, and that provision must specifically authorize disclosure of the personal information.

A *treaty* is a formally concluded and ratified agreement between or among independent states. Only the federal government of Canada has the power to conclude treaties with foreign countries. An example of a treaty permitting the exchange of personal information is the *Mutual Legal Assistance Treaty*, which provides for the exchange of information on a variety of law enforcement matters.

An *arrangement* is a coming to terms on how certain matters will be conducted. Arrangements should, whenever possible, be in writing. A verbal arrangement should be allowed only in very exceptional circumstances, such as sensitive law enforcement, security or intelligence matters, and only at the insistence of one or more of the parties. Where an arrangement is unwritten, disclosures should be approved at a senior level within the public body.

An *agreement* is similar to an arrangement but is more precise in setting out the actions to be taken. *All agreements should be in writing.*

Agreements concerning the disclosure of personal information by public bodies to other organizations, including federal, provincial, municipal, and foreign governments and international bodies, should contain:

- **a description of the personal information to be shared;**
- **the purposes for which the information is to be shared and used;**
- **a statement of all the administrative, technical and physical safeguards required to protect the confidentiality of the information, especially with respect to its use and disclosure;**
- **a statement specifying whether information received by a public body will be subject to the provisions of the *FOIP Act* or, for other jurisdictions where comparable legislation exists, whether that legislation will apply;**
- **a statement that the sharing of the personal information shall cease if the recipient is discovered to be improperly disclosing the shared information; and**
- **the names, titles and signatures of the officials in both the supplying and receiving public bodies who are responsible for the terms of the agreement, the date of the agreement and the period for which it is in effect.**

Examples of such agreements include agreements on:

- the exchange of personal information about people who have applied for social assistance from the Province with Human Resources Development Canada to determine whether they are also receiving employment insurance;
- the exchange of information about applicants for the Alberta Seniors Benefit with Alberta Health and Wellness so that applicants can obtain seniors' health benefits; and
- the provision of information by schools to health authorities for the purpose of immunization and other preventive health services.

For further information, see Chapter 9.6 of this publication and *Freedom of Information and Protection of Privacy: Guide to Developing Personal Information Sharing Agreements*, produced by Information Management and Privacy, Alberta Municipal Affairs.

***Disclosure in accordance with an enactment of Alberta or Canada that authorizes or requires disclosure* (section 38(1)(e)):** This provision is related to **section 38(1)(d)**. However, whereas in **section 38(1)(d)** disclosure must be *for the purpose of complying* with an enactment, and is therefore likely to be required by law, in **section 38(1)(e)**, disclosure is permitted if it is either required or *authorized* by an enactment of Alberta or Canada. If disclosure of personal information is authorized – but not required – by an enactment, the head of the public body has more discretion as to whether or not to disclose the information.

Examples of Acts that require disclosure of personal information include the *Legislative Assembly Act* and the *Public Lands Act*. Examples of Acts that authorize disclosure of personal information include the *Charitable*

Fund-Raising Act and the *Dependent Adults Act*.

***Complying with a subpoena, warrant or order* (section 38(1)(f)):** This provision permits personal information to be disclosed in order to comply with legal processes that require the production of information. These processes include the use of a subpoena, warrant or order issued or made by a court, person or body having jurisdiction to compel the production of information or with a rule of court that relates to the production of information.

A *subpoena*, also called a "summons to witness," is a command issued by a party in litigation requiring the attendance of someone as a witness at a court or hearing. It will specify a certain place and time when testimony on a certain matter will be required, and may also order a person to meet the requirements of a court to disclose information.

Time is usually of the essence in dealing with a subpoena, as it is often served with very little notice. Public bodies cannot ignore subpoenas since they would risk being cited for contempt of court and, at a minimum, fined.

A *warrant* is a judicial authorization to collect information – in this context, personal information.

An *order* is an authoritative command, direction or instruction to produce something – again in this context, personal information.

Although **section 38(1)(f)** is permissive in nature, public bodies normally comply with orders, warrants or subpoenas because they are required by law to do so and generally wish to assist the administration of justice.

Public bodies should consult their legal advisor when they receive an order, warrant or subpoena in order to determine whether it refers to information that is actually in the custody or under the control of the public body, whether the instrument has been served properly and whether there is some compelling reason to oppose the order, warrant or subpoena.

***To an officer or employee of the public body, or to a member of Executive Council* (section 38(1)(g)):** This provision permits disclosure to officers or employees of the public body that has custody or control of the personal information and to Cabinet members. **It *does not* allow disclosure to employees or officers of *other* public bodies.**

An *employee* is a person employed by a public body. The definition in **section 1(1)(e)** of the *Act* includes a person retained under contract to perform services for the public body, a volunteer and an appointee to a board or committee.

The term *officer* is included to ensure that all persons working for a public body in any capacity are encompassed by the provision. This includes an elected official, such as a school board trustee, when acting on behalf of the public body to carry out the mandate and functions of the public body, as opposed to functioning as a representative of his or her constituents (see *IPC Order 99-032*).

A *member of the Executive Council* includes the President of Executive Council, a Minister, and an Associate Minister (described in the *Legislative Assembly Act* as a "Minister without Portfolio").

The provision does not allow an official or employee or member of the Executive Council automatic access to all personal information within a public body. **The test for disclosure is whether the information is *necessary for the performance of duties.*** Disclosure is permissible only if access to the particular personal information is needed to do a job or deal with a particular situation.

The persons to whom the information is disclosed should be able to prove a need to see, generate or handle the personal information in order to do their jobs.

Examples of cases where disclosure might be necessary for the performance of an employee's duties include the following:

- a staffing team requires access to the resumes of applicants in order to carry out the recruitment function;
- a service counter team needs to be informed if a client has a history of acting violently when interacting with departmental staff and if there is a need for extra security when the individual approaches the office;
- a counsellor requires access to student records to provide assistance, at the request of a teacher, to a student who is not doing well in school;
- the head of a local public body requires information to prepare a report for the governing body; and
- a Minister needs background information about an issue and the people he or she is meeting in order to understand the problem and their needs.

***For the delivery of a common or integrated program or service* (section 38(1)(g.1)):** This provision has the same requirements as **section 38(1)(g),** but permits disclosure to officers or employees of *another* public body. This is permitted when two or more public bodies are working together to provide or deliver a common program or service.

Section 38(1)(g) does not allow disclosure to an organization that is not a public body.

Common means that there is a single program or service that is provided or delivered by two or more public bodies.

Integrated means that the program has several distinct components, each of which may be provided or delivered by separate public bodies, but those components together constitute the program or service.

This provision allows for the sharing of personal information between the service providers in order to deliver the service to the clients. A common client does not, of itself, meet this definition. Factors that will determine whether or not a program or service meets the definition include:

- evidence of joint planning;
- a formal agreement or legislative authority for working together;
- common goals expressed by the partners; and

- evidence of collaboration or cooperation in delivery.

When public bodies are implementing such programs or services, they should:

- ensure that individuals participating in the program are notified of all the partners and of the sharing of personal information;
- disclose information in non-identifiable form whenever possible;
- disclose personal information only to those who need to know about a particular individual;
- disclose personal information only to the extent necessary for program or service delivery; and
- ensure that personal information is not used for any other purpose.

Examples of such programs and services include:

- children's service initiatives delivered through Child and Family Service Authorities;
- conjoint nursing programs that require the disclosure of personal information between program departments;
- work placement and practicum programs;
- school-housed public libraries; and
- centralized human resource programs.

For further information, see *FOIP Bulletin No. 8, Common Programs and Services.*

***To enforce a legal right of the Government of Alberta or a public body* (section 38(1)(h)):** This provision permits the disclosure of personal information to enforce a legal right that the Government of Alberta or a public body has against any person.

In most cases, the disclosure of personal information under this provision will be to the legal representatives of a public body or, in the case of provincial public bodies, to Alberta Justice as the provincial government's legal representative. The legal rights may relate to civil or criminal law.

***Collecting a fine or debt or making a payment* (section 38(1)(i)):** This provision permits disclosure of personal information to:

- collect a fine or debt owing to the Government of Alberta or a public body or an assignee of either of them; or
- make a payment owed by the Government of Alberta or a public body.

This provision enables public bodies to exchange personal information with other public bodies and outside agencies to locate an individual and collect a fine or debt or in order to make a payment.

It *does not* permit information to be exchanged between public bodies for the purpose of determining whether a fine, debt or a benefit is owed. This decision must be made before the information is disclosed.

The provision permits disclosure to a private collection agency to which the debt has been assigned. It does not permit disclosure to assist such a collection agency, or any other person or organization that is not a public body, to collect a debt owed to a person or organization that is not a public body.

Documentation requesting disclosure under this provision should be in writing and specify:

- **the nature of the information to be disclosed;**
- **the name of the public body, person or organization receiving the information;**
- **any other necessary identifying information such as a case or file number;**
- **the purpose of the request, including a citation of the legal authority for collecting the fine or debt; and**
- **the name, title and business address of the official making the decision to disclose.**

The information disclosed should be the minimum needed to enable the collection or payment to be made. Usually this will be the name, last known address and telephone number, and any contact information provided by the individual. **Disclosure should always be in writing.**

A *fine* is a monetary punishment imposed on a person who has committed an offence, including an offence under a by-law.

A *debt* is something that is owed, usually money, where the individual has an obligation to pay and the creditor has the right to receive and enforce payment.

This provision is intended to assist public bodies in cases where their legislative mandate does not specifically extend to the collection of fines and debts. It gives them an authority under which to pursue these activities. Many public bodies already have authority to collect fines and debts in their legislation.

***Determination or verification of suitability or eligibility for a program or benefit* (section 38(1)(j)):** This provision permits the disclosure of personal information to determine an individual's suitability or eligibility for a program or benefit, or to verify continuing eligibility for the program or benefit.

Section 38(1)(j) allows personal information to be disclosed when there is a need to determine whether or not an individual meets the eligibility or suitability criteria for a particular program or benefit. The information must have been collected or compiled by a public body. Disclosure may be made to any organization or institution that needs such verification information; it is not limited to another public body.

Normally, disclosure will only be made after an application has been made by an individual to participate in a program or for a benefit. Public bodies collecting such information should comply with the guidelines set out in section 7.3 of this chapter.

Eligibility means the state of being qualified or permitted to be chosen for a program or benefit.

Suitability means the characteristics of an individual that enable him or her to be chosen for a program or benefit. Examples of disclosures that might be permitted under this provision include:

- verification of employment information when someone applies

for employment insurance or employment counselling;
- disclosure of information from a seniors' lodge to a health authority to determine suitability for nursing home care;
- confirmation of membership in a library when an individual uses his or her library card in another library; and
- provision of information on attendance or marks to enable a second year of grant support to a student.

***Audit purposes* (section 38(1)(k)):** This provision permits the disclosure of personal information to the Auditor General and to other persons and bodies established by regulation for audit purposes.

The *Auditor General* is an Officer of the Legislature appointed by the Lieutenant Governor in Council. The role of the Auditor General is to examine the accounts and records of the Government relating to the consolidated revenue fund and all public money, including trust and special funds under the management of the Government and relating to public property. The Auditor General must report annually to the Legislature on his or her work, including findings as to whether or not departments and public bodies have carried out their financial responsibilities. **This provision does not apply to the Auditor General of Canada.**

For audit purposes means for the purposes of the examination of accounts, including value-for-money audits that examine revenues, expenditures and public policy approaches. It does not include the verification of a claimant's eligibility for a program, benefit or service, where an actual decision would be taken about an individual.

The persons to whom personal information may be disclosed for audit purposes are specified in **section 7** of the FOIP Regulation. Disclosure can be made to persons who are employees of a public body, including a person retained under contract to perform services for the public body. Personal information may be disclosed in order to carry out a financial or other formal and systematic examination or review of a government program, portion of a program or an activity that includes personal information.

Such an audit must be sanctioned by statute, regulation or public policy relating to the public body. In the case of a local public body, this means that the audit may be sanctioned by by-law or resolution.

When a contractor is hired to conduct an audit requiring disclosure of personal information under this provision, the contractor should be advised of, and agree to abide by, the provisions of the *FOIP Act*, as well as policy relating to the protection of privacy under the *FOIP Act*.

Information disclosed under **section 38(1)(k)** is only to be used for audit purposes and not for operational or administrative purposes involving the individuals concerned.

Examples of disclosures that may be permitted under this provision include:

- disclosure to the internal auditors of a municipality;

- disclosure to an accounting or audit firm engaged to conduct a financial audit of a public body;
- disclosure to a person auditing methods of determining how a housing management body determines eligibility for low income housing; and
- disclosure for personnel audits, such as classification reviews or quality assurance audits of the work being performed.

***Disclosure to a Member of the Legislative Assembly* (section 38(1)(l))**: This provision permits disclosure of personal information to a Member of the Legislative Assembly who has been requested by the individual the information is about to assist in resolving a problem.

A *Member of the Legislative Assembly* (MLA) is a person elected as a representative of a constituency within the province of Alberta to represent the interests of the voters in that constituency in the Legislative Assembly.

This provision permits disclosure only to Members of the Legislative Assembly of Alberta, not to those working for them, and only to assist the person concerned to resolve a problem.

The provision *does not* permit the disclosure of personal information to federal Members of Parliament or municipal representatives. These representatives may, however, obtain personal information about an individual with his or her consent.

The purpose of disclosure under **section 38(1)(l)** must be to *assist in resolving a problem*. This includes helping an individual to provide information to a public body, inquiring about decisions or about a service or benefit, or correcting a mistake or misunderstanding. Where resolution of the problem is relatively straightforward, the public body can discuss the issue with the MLA and, with his or her agreement, simply call the individual concerned and provide the information directly.

The written consent of the individual concerned is not normally necessary for disclosure to MLAs under this provision. If possible, the inquiry and disclosure should be recorded in writing. Where inquiries and disclosures take place orally, the transactions should be noted on the person's file.

In cases where the information is particularly sensitive (e.g., medical, financial or law enforcement information), the public body may wish to obtain the written consent of the individual concerned before releasing the information.

Public bodies should have a policy in place for disclosure of such information and should inform MLAs of their policy if a request is received for information.

It is likely that the MLA will pass the personal information he or she receives from a public body to the person concerned. Public bodies should bear in mind the exceptions to the right of access set out in **Part 1** of the *Act* when deciding what it is and is not appropriate to disclose under this provision.

***Representative of a bargaining agent* (section 38(1)(m))**: This provision permits disclosure of personal information to a bargaining agent who has been authorized in writing by the employee the information is about to make an inquiry.

This provision permits disclosure to a representative of a union or other organization that negotiates on behalf of workers with their employers for improvements in pay, hours, benefits, and other working conditions, and that works to protect the rights of employees.

The individual must sign and date a statement of authorization or representation clearly stating to whom the information may be disclosed and for what purpose.

Disclosure is limited to personal information that is necessary for the purpose of *making an inquiry* and the representative may receive only that personal information that the employee has specifically authorized for release.

The representative, unless duly authorized as the employee's representative, may not exercise the employee's right of access to the rest of his or her personal information. Nor can he or she exercise the right to request correction of the employee's personal information.

Public bodies should ensure that their employees understand the purposes of the *Act* with respect to protection of personal information and the way the *Act* is applied in circumstances where a bargaining agent requests information about an employee.

***Disclosure for archival purposes* (section 38(1)(n)):** This provision permits disclosure of personal information to the Provincial Archives of Alberta or the archives of a public body for permanent retention.

The archives of a public body means:

- a public body's own archives, in which case the records will remain in the custody or under the control of that public body (e.g., the archives of most post-secondary institutions);
- the archives of another public body, to which records are transferred as authorized under **section 3(e)**, in which case custody and control of the records will normally be transferred to the archives; or
- an archival facility that operates under a contract or agency relationship with the public body (e.g., the Glenbow-Alberta Institute), in which case custody may be transferred but control must be retained by the public body.

This provision does not permit disclosure to private archives such as those run by a private museum or historical society.

Section 38(1)(n) permits the disclosure of personal information to the personnel of the archives:

- during the records scheduling process, to determine what personal information may have long-term archival and historical value, and
- after the transfer and deposit of the records in the Provincial Archives or the archives of a public body, for ongoing research purposes.

Further disclosure by archives is governed by **section 41** of the *Act*. See section 7.11 of this chapter for a discussion of **section 41**.

***Assistance to law enforcement* (section 38(1)(o)):** This provision permits the disclosure of personal information to a public body or a law enforcement agency in Canada to assist in an investigation:

- undertaken with a view to a law enforcement proceeding; or
- from which a law enforcement proceeding is likely to result.

Law enforcement is defined in **section 1(1)(h)** of the *Act* and further explained in Chapter 4.7 of this publication.

A *law enforcement agency in Canada* includes a variety of agencies that are responsible for enforcing statutes. Examples of such agencies are Alberta Justice (see *IPC Order 96-007*), the RCMP, provincial, municipal and First Nations' police services, the Coordinated Law Enforcement Unit (CLEU), Revenue Canada, the Alberta Securities Commission, fire commissioners' offices, conservation services and the Superintendent of Financial Institutions.

Public bodies should not disclose personal information when the law enforcement agency cannot provide definite and focused investigative information as to why disclosure is needed. Personal information should not be disclosed on the basis that there is a suspicion, surmise or guess that it may be useful to an investigation.

A request by a law enforcement agency for personal information should be in writing and should be retained by the public body as a record of whether or not the disclosure occurred.

Public bodies should ensure that requests for personal information from law enforcement agencies are justified and contain:

- the name of the individual whose information is requested;
- the exact nature of the information desired;
- the authority for the investigation;
- the purpose for which the requesting agency will use the information; and
- the name, title and address of the person authorized to make the request.

A model **Law Enforcement Disclosure Form** is provided in Appendix 6 of this publication. Law enforcement agencies are encouraged to use this or a similar form when requesting disclosure of personal information.

The record of disclosure should normally be kept in a separate file that documents all requests for disclosure from law enforcement agencies, since this record may itself qualify for exception under **section 19** of the *Act*.

An *investigation* is a methodical process of examination, inquiry and observation. Examples of investigations include the examination of crime scenes, the interviewing of witnesses and the amassing of evidence, all of which tend to generate recorded information on the matter under investigation.

To use this provision, the investigative process must be with a view to, or likely to lead to, law enforcement proceedings. However, there does not have to be a guarantee that the proceedings are actually going to occur and, indeed, they could be suspended for many reasons, including lack of evidence.

Proceeding means an action or submission to any court, judge or other body having authority, by law or by consent, to make decisions concerning a person's rights. In this context, it includes administrative proceedings before agencies, boards and tribunals if the proceedings could lead to a penalty or sanction, including a penalty or sanction imposed by another body to which the results of the proceeding may be referred.

A *law enforcement proceeding* has as its purpose the imposition of penalties or sanctions, as opposed to the gathering of information for criminal or security intelligence purposes.

Section 38(1)(o)(ii) limits the discretion to disclose personal information with the requirement that, at a minimum, the disclosure of personal information must be to assist an investigation from which a *law enforcement proceeding is likely to result*. When disclosure is contemplated before an actual law enforcement proceeding is under way, there must be a probability that a law enforcement proceeding will go forward.

***Disclosure among law enforcement agencies* (section 38(1)(p)):** This provision permits a public body that is a law enforcement agency to disclose personal information:

- to another law enforcement agency in Canada; or
- to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority.

This provision permits law enforcement agencies in Alberta to exchange personal information with their federal, provincial and municipal counterparts in Canada. Examples include the RCMP, provincial securities commissions and other police services.

As well, the provision deals with *law enforcement agencies in foreign countries*. This includes police forces and other law enforcement organizations in other countries, international law enforcement organizations and municipal and state police forces in foreign countries. Examples would be the Metropolitan Police in England, the Federal Bureau of Investigation and the United States Immigration and Naturalization Service in the United States, and Interpol.

Disclosures under **section 38(1)(p)(ii)** must be made in accordance with an arrangement, written agreement treaty or legislative authority. The same conditions for an arrangement, agreement or treaty prevail as for **section 38(1)(d)** described above.

Legislative authority means a statute, regulation or other legislative instrument.

***Notification in case of injury or sickness* (section 38(1)(q)):** This provision permits disclosure of personal information so that a spouse, relative or friend of an injured, ill, or deceased individual may be contacted.

It would also allow disclosure of such personal information as whether the individual has been taken to a hospital or requires assistance to get home.

***In accordance with sections 40 or 41* (section 38(1)(r)):** This provision permits the disclosure of personal information for research and statistical purposes. The conditions applicable to research disclosures are discussed in sections 7.10 and 7.11 of this chapter.

***Disclosure to an expert under section 17(2)* (section 38(1)(s)):** This provision permits disclosure of personal information to an expert as provided for in **section 17(2)** of the *Act*. It allows the expert to determine whether or not release of the applicant's own information to the applicant could reasonably be expected to result in immediate and grave harm to the applicant's health or safety.

Section 5 of the FOIP Regulation establishes conditions for such disclosure of personal information to a physician, chartered psychologist, psychiatrist or other expert as follows:

- the public body may disclose information relating to the mental or physical health of an individual to a medical or other expert for an opinion on whether disclosure of this information could reasonably be expected to result in grave and immediate harm to the individual's safety or mental or physical health;
- a medical or other expert to whom information is disclosed must not use the information except for the purposes of determining the harm described above;
- the public body must require a medical or other expert to whom the information will be disclosed to enter into an agreement relating to the confidentiality of the information; and
- if a copy of the record containing information relating to the mental or physical health of an individual is given to a medical or other expert for examination, the medical or other expert must, after giving the opinion, return the copy of the record to the public body or dispose of it in accordance with the agreement between the public body and the expert.

***Court or quasi-judicial proceedings* (section 38(1)(t)):** This provision permits disclosure of personal information for use in a proceeding before a court or quasi-judicial body to which the Government of Alberta or a public body is a party.

It permits the disclosure of personal information to the legal representatives of the Government of Alberta or a public body for use in such proceedings. It also permits disclosure to the members of the quasi-judicial body or court.

Disclosure is normally to, or through, the legal representative of the public body or, in the case of provincial public bodies, Alberta Justice, which represents the provincial government in legal matters. Such information may be disclosed to the legal representative of the other parties to a proceeding in accordance with the court disclosure and discovery rules that apply.

For more information about quasi-judicial bodies see Chapter 1.7 of this publication.

***Disclosure to a place of lawful detention* (section 38(1)(u)):** This provision permits the Minister of Justice and Attorney General or an agent or lawyer of that Minister to disclose personal information in the custody or under the control of that department. The information may be disclosed to a place of lawful detention in order to provide for the appropriate supervision of any individual detained in custody.

***Management of personnel* (section 38(1)(v)):** This provision allows government departments and public bodies subject to the *Public Service Act* to disclose personal information about an employee or prospective employee to each other. The provision recognizes the provincial government as the employer for all provincial departments.

The provision allows other public bodies to disclose the same kind of information only *within* the public body that has custody and control of the information.

No disclosure is permitted to other public bodies or the private sector without the written consent of the individual unless some other provision of section 38 permits it.

Management or administration of personnel includes all aspects of the management of human resources of a public body. This includes the operations relating to human resources of the government-wide network managed through the Personnel Administration Office. It includes staffing, job classification, recruitment and selection, salary and benefits, hours and conditions of work, leave management, performance review, training, separation and layoff.

Employees should be informed, in a general way, of how they should expect their personal information to be collected, used and disclosed within the personnel management system.

Disclosure of personal information for the purposes of the management or administration of consultant, professional or other personal services contracts should be addressed in the terms of the contracts.

Disclosures under this provision are permitted only within the official framework that governs the management and administration of personnel within a public body or across the Government of Alberta.

Disclosure of personnel information is discussed in more detail in a publication produced for local public bodies by Information Management and Privacy, Alberta Municipal Affairs. This publication is entitled *Human Resources Guide for Local Public Bodies*.

***Enforcement of maintenance orders* (section 38(1)(w)):** This provision permits the disclosure of personal information about individuals for the purposes of enforcing a maintenance order under the *Maintenance Enforcement Act*.

Public bodies should disclose only personal information that is relevant to the enforcement process relating to the order.

Disclosure can take place only to the Director of Maintenance Enforcement or someone delegated to act on his or her behalf.

***Disclosure to an Officer of the Legislature* (section 38(1)(x)):** This provision permits the disclosure of personal information to an Officer of the Legislature if the information is necessary for the performance of the duties of that officer. Officers of the Legislature are the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner and the Information and Privacy Commissioner (**section 1(1)(m)** of the *Act*).

Disclosure under **section 38(1)(x)** is restricted by the requirement that the information is necessary for the performance of the Officer of the Legislature.

If the reason for the disclosure is not clear from the request, public bodies should seek an explanation as to why the personal information is needed.

Information may be disclosed under this provision for the purpose of a review of a privacy complaint by the Information and Privacy Commissioner, or an investigation by the Ombudsman at the request of an individual.

***Supervision of an individual by a correctional authority* (section 38(1)(y)):** This provision permits the disclosure of personal information about an individual for the purpose of supervising the individual while he or she is under the control or supervision of a correctional authority.

Supervision includes any community disposition requiring supervision of an offender, including probation, bail supervision, parole, temporary absence, and ordered community service work, as well as supervision of individuals held in a correctional institution.

***Disclosure of information available to the public* (section 38(1)(z)):** This provision permits personal information to be disclosed when that information is available to the public. It applies to information that has been published in any form or which constitutes or is a part of a record that is publicly available.

The provision covers situations where a public body wishes to obtain personal information that is in the public domain from another public body, as well as disclosure to the public or to a private-sector organization.

It is important, however, to assess carefully just how public the information is. For example, just because personal information about an individual has been published in the media does not mean that the information should automatically be treated as public and disclosed freely. If a public body is contemplating making this type of disclosure, it should take into consideration the possibility that the individual involved might still find such disclosure an unreasonable invasion of his or her privacy (see *IPC Order 99-032*).

Examples of public information that might be disclosed under this provision include:

- individual employee information in a corporate telephone directory available for purchase or freely available on the Internet;
- biographical information about board appointees published in a newsletter;
- details of a personal contract approved in a council meeting;
- retirement details of a school superintendent mentioned in board minutes; and
- information in court decisions published in law reports (see *IPC Order 98-001*).

***Disclosure to a relative of a deceased person* (section 38(1)(aa)):** This provision permits personal information to be disclosed to a relative of a deceased individual if that disclosure is not an unreasonable invasion of the deceased individual's personal privacy.

Privacy for a deceased individual normally endures for a period of 25 years (see **section 16(2)(i)**).

Section 38(1)(aa) permits a public body to disclose information earlier to a relative. A *relative* in this context means a spouse, child, parent, brother, sister, or anyone else that can prove a family relationship with the deceased.

Evidence of the relationship of the person to the deceased individual should be produced before personal information is disclosed. This should consist of reliable documentation of the relationship (e.g., a birth or marriage certificate). As well, if a public body is not certain that the individual is deceased, the person seeking disclosure must provide reliable evidence that the individual is dead (e.g., a death certificate or obituary).

This provision recognizes that the privacy interests of an individual generally diminish with the passage of time, and that there may sometimes be a need for relatives to have access to information about deceased family members to resolve personal matters or advance individual rights.

The constraining factor in the provision is the *unreasonable invasion of privacy* test relating to the deceased individual. In considering disclosure, the public body should weigh the sensitivity of the information against the interest of the relative in having access to the information. The need of the relative should go beyond mere curiosity about the deceased individual. For more information on making a decision, see Chapter 4.4 of this publication.

Particularly important factors to consider are whether:

- the personal information was supplied in confidence;
- the disclosure is desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny;
- the personal information is relevant to a fair determination of the requesting individual's rights;
- the personal information was originally supplied by the requesting individual;
- disclosure may endanger the physical or mental well-being of any other living member of the family;
- there are grounds to believe that another member of the family does

not want the information disclosed to the relative;

- the personal information is likely to be inaccurate or unreliable;
- the information contains medical, psychological or social work case reports or data which it is reasonable to believe would prove harmful to familial relationships; and
- disclosure may harm the reputation of the deceased, who cannot defend him or herself.

***Legal representative of inmate* (section 38(1)(bb)):** This provision permits the disclosure of personal information to a lawyer or student-at-law who is acting for an inmate under the control or supervision of a correctional authority.

For information on *supervision* see the discussion on **section 38(1)(y)** above.

***Disclosure to avert danger to health or safety* (section 38(1)(cc)):** This provision permits disclosure when a public body has reasonable grounds to believe the disclosure will avert or minimize a serious health or safety risk to any person. The danger has to be imminent.

Imminent danger means a danger that is likely to arise immediately or very soon.

A public body will have to consider all the information in its possession about an individual when making a decision. Past behaviour of the individual is one factor that may assist in decision-making.

Examples of information that might be disclosed under this provision include:

- information about the escape or release of a violent offender to a past victim; and
- information about a student's threat of suicide to residence supervisors on a college campus.

***Administration of the Motor Vehicle Accident Claims Act* (section 38(1)(dd)):** This provision permits disclosure of personal information to the Administrator of the *Motor Vehicle Accident Claims Act* or to an agent of lawyer of the Administrator.

It is intended to allow the Administrator to deal with claims made under that Act. It permits police services and other public bodies, such as Alberta Infrastructure, to disclose any information gathered about an accident to the Administrator once a claim has been lodged.

***Disclosure of alumni records for fund-raising purposes* (section 38(1.1)):** This provision permits post-secondary educational institutions to disclose information in their alumni records for the purposes of their own fund-raising activities.

Disclosure may be made to any person acting on behalf of the post-secondary institution in raising funds. This includes alumni associations, foundations, private fund-raising organizations, and other persons raising funds on behalf of the institution.

The person to whom the disclosure is made must have a written agreement with the post-secondary institution. The agreement must:

- allow individuals a right of access to their own personal information disclosed under the agreement, and
- provide that the person using the information will discontinue using that information if an individual so requests.

The agreement should also contain other clauses to ensure compliance with the privacy protection provisions of the *Act*.

This provision complements the provision in **section 37(2)**, as outlined in section 7.7 of this chapter.

***Teaching and course evaluations* (section 38(1.2)):** This provision permits disclosure of personal information contained in student evaluations of instructors and courses at post-secondary educational institutions.

Disclosure is limited to evaluations completed by students. It does not extend to evaluations of courses by faculty members.

The amount of personal information disclosed is limited to that which would assist a student in selecting courses. If the evaluation includes information not relevant to selection of a course, it would have to be severed before disclosure.

Post-secondary educational bodies should ensure that information that is disclosed is valid and up-to-date, and should establish written policies to ensure that the practice is carried out in a responsible manner.

7.9 CONSISTENT USES

Section 39 of the *Act* provides that for the purposes of **sections 37(1)(a)** and **38(1)(b)**, a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure:

- has a reasonable and direct connection to that purpose; and
- is necessary for performing the statutory duties of or for operating a legally authorized program of, the public body that uses or discloses the information.

Section 39 balances the protection of individuals' privacy against the need of public bodies to use and disclose personal information effectively to carry out program activities and fulfil their legislated mandates.

Section 37(1)(a) allows a public body to *use* personal information for a purpose that is consistent with the purpose for which the information was originally collected.

In most cases the public body using the information will be the public body that collected it. However, if the personal information has been collected for the purposes of delivering a common or integrated program or service, the public body using the information may not be the public body that originally collected it.

See section 7.8 of this chapter for further information on common or integrated programs and services (**section 38(1)(g.1)**).

Section 38(1)(b) allows a public body to *disclose* personal information for a purpose that is consistent with the purpose for which the information was originally collected. In most cases this provision will apply to disclosure outside the public body.

The new use or disclosure must be consistent with the purpose for which the information was collected or compiled.

A use or disclosure has a *reasonable and direct connection* to the original purpose if there is a logical and plausible link to the original purpose. A new use should grow out of or be derived from the original use.

A use or disclosure is *necessary for performing the statutory duties of, or for operating a program of, the public body* if the public body would be unable to carry out its program without using or disclosing the personal information in the way proposed.

A consistent use or disclosure must meet both of the above conditions to be valid.

Examples of Use for Consistent Purpose

***Evaluation of a program*:** Public bodies will have a regular need to evaluate the operation and success of their programs. This is particularly true of new programs or those that have changed in some way. This provision allows a public body to select clients or participants who can participate in that evaluation through questionnaires or interviews.

***Verification of ownership*:** Local government bodies issue permits for such things as development of a property, demolition and burning. These permits are issued to the owner of a property. This provision allows staff who approve the permit to verify ownership from the assessment roll.

***Expansion of a program*:** Public bodies set criteria for participation in programs. If the criteria are broadened, people who were originally rejected may become eligible. This provision allows a public body to determine eligibility on the basis of the original submissions from these people rather than collecting the information again.

Public bodies are required to maintain a record of all uses of personal information, including all consistent uses, in order to be able to provide complete, current and accurate descriptions of the personal information banks in their custody or under their control for the use of the public (section 82(3)).

7.10 DISCLOSURES FOR RESEARCH OR STATISTICAL PURPOSES

Section 40 of the *Act* enables a public body to disclose personal information for a research purpose, including statistical research, only if:

- the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form or the research purpose has been approved by the Information and Privacy Commissioner;

- any record linkage is not harmful to the individuals the information is about and the benefits to be derived from the record linkage are clearly in the public interest;
- the head of the public body has approved conditions relating to the following:
  - security and confidentiality,
  - the removal or destruction of individual identifiers at the earliest reasonable time,
  - the prohibition of any subsequent use or disclosure of the information in individually identifiable form without the express authorization of that public body;

  and
- the person to whom the information is disclosed has signed an agreement to comply with the approved conditions, the *FOIP Act* and any of the public body's policies and procedures relating to the confidentiality of personal information.

The provision enables research to take place while at the same time ensuring that privacy is protected. This is accomplished by the strict conditions set out above. For a research project to be considered under this provision *all four requirements must be met*.

For a research purpose means for the purpose of a systematic investigation or study of materials or sources in order to establish facts or to verify theories.

Statistical research is research based on the collection and analysis of numerical data using, in this case, quantifiable personal information to study trends and draw conclusions.

Individually Identifiable Information

Information is in *individually identifiable form* if unique identifiers are attached to the information such that the information clearly pertains to a particular person. The identifiers might be an individual's name, address, telephone number, date of birth, social insurance number or personal health number.

Section 40(a) makes provision for situations where:

- the research purpose cannot reasonably be accomplished unless the information is provided in individually identifiable form; or
- the research purpose has been approved by the Information and Privacy Commissioner.

The first part of this provision allows public bodies to disclose personal information for research in circumstances where the research cannot be completed without access to the information in individually identifiable form.

This might be the case where, for example, there is no intention to use individually identifying information in the research but it would be impractical to sever the personal information because of the volume of the records, the intertwined nature of the personal information or time constraints on the research project.

The second part of the provision allows public bodies to disclose personal information for research if the Information and Privacy Commissioner has approved the research purpose. Approval by the Commissioner ensures that the research purpose is subjected to impartial scrutiny.

In this case, the researcher would submit the proposal to the Commissioner in writing, clearly explaining the nature of the research, the information involved and the reason for the request that he approve the research.

Record Linkage

Section 40(b) places controls on any record linkage performed during a research project.

Record linkage is a form of data matching involving the systematic comparison of sets of information, often personal information, to establish relationships among data. Within the research context, it often involves the creation of a new database allowing the statistical correlation of research variables. Record linkage can be a useful tool for quantitative analysis in research projects.

Record linkage for research purposes is the matching of sets of personal information to achieve the objectives of the research project, with no intention of making decisions about the research subjects' rights or privileges. The matching is a means of linking the right information to the right people in a representative sample used in a study. This makes it distinct from the kind record linkage for individual *profiling* that is used in some marketing strategies, for example.

Record linkages permitted under section 40 are only for research purposes and no decision that directly affects an individual may be made as a result of such linkage.

The provision also requires that a linkage *not be harmful*. This means that a linkage must not have an adverse affect on the individuals under study – that is, the information disclosed must not result in damage to an individual's reputation, or denial of a job, benefit or service.

Finally, linkages need to be considered in terms of the *benefits derived* from them. The benefits of the research and linkage must override the invasion of privacy that occurs with the disclosure of personal information to the researcher. The research and linkage must be *clearly in the public interest*. That is, the benefits must apply to a wide public and not to just one or two individuals.

Approval of Conditions

Section 40(c) provides that a disclosure for research purposes may take place only if the public body is aware of and has approved the researcher's proposed practices for handling personal information.

Security refers to the physical protection or guarding from unauthorized access or disclosure, theft or other danger of the personal information used in a research project.

Good security may require such measures as locked filing cabinets, computer controls and access codes, restricted work areas, and encryption or encoding of data, depending on the sensitivity of the data involved and the threat and risk associated with it.

Confidentiality means keeping personal information private and safe from unauthorized access, use or disclosure. It means that there is no disclosure, orally or otherwise, other than to those working on the project. For sensitive personal information, disclosure should be on a "need-to-know" basis.

Removal or destruction of individual identifiers means the deletion of identifying information, such as name, address, social insurance number or other numerical identifier, or the destruction of the identifiers in whatever way is appropriate to the medium on which the information is stored. This must be done in such a way as to render the information anonymous.

Removal of identifiers is to take place at *the earliest reasonable time*. This will vary with the circumstances of the case and the comparisons the researcher is making between different sets of data. However, the researcher and the public body should agree on a specific date when a researcher can strip off all identifiers because all the different sets of information have been combined and are ready for analysis.

Prohibition on any subsequent use or disclosure means a prohibition on any further use or disclosure of the personal information by the researcher for any purpose, including any other research or statistical purpose. It can only be used for the project for which the information was originally disclosed, unless the public body explicitly authorizes another research use. This prohibition includes a ban on the use of the information to sell products or services to the subjects of the study and a ban on the sale or gift of the information to a charity in order to help solicit donations.

Agreement to Comply with Approved Conditions

Section 40(d) provides that the researcher must sign a detailed research agreement. This agreement must include all the provisions set out in **section 8** of the FOIP Regulation:

- personal information disclosed can only be used for a research purpose set out in the agreement or for which written authorization has been given by the public body;
- the names of those persons who will be given access to the personal information must be provided;
- the researcher must bind these persons, through an agreement, to adhere to the same conditions as the researcher;
- information must be kept in a secure location;
- how and when the identifiers will be removed or destroyed must be specified;
- contact with the individuals to whom the information relates is prohibited without prior written authority from the public body;
- no use or disclosure can be made of the information in a form that identifies individuals without prior written authorization from the public body;
- information cannot be used for an administrative purpose directly affecting an individual;
- notification is required if any conditions of the agreement are breached; and
- failure to meet the conditions may result in cancellation of the

agreement and leave the researcher open to charges under **section 86(1)** of the *Act*.

The model **Proposal for Access to Personal Information for Research and Statistical Purposes Form** and the related **Agreement** in Appendix 6 are suitable for an individual or group of researchers that is not part of any public body. If another public body proposes research, a Personal Information Sharing Agreement would likely be more appropriate (see Chapter 9.6 of this publication).

7.11 DISCLOSURE OF INFORMATION IN ARCHIVES

Section 41 provides for the disclosure of information without a FOIP request by the Provincial Archives of Alberta or the archives of a public body, including those of a post-secondary educational body.

This section is intended to support research by allowing access to archival holdings for research, subject to a limited number of restrictions. Like **section 38**, **section 41** is *enabling*. It *permits* the archives to disclose information *under specified conditions*; it does not *require* the archives to disclose information.

The section does not apply to records that were unrestricted before the *FOIP Act* came into force **(section 3(b))**.

Section 41(1) applies to all public body archives, including the archives of post-secondary educational bodies. **Section 41(2)** applies only to the archives of post-secondary educational bodies.

Effect of Other Acts

Section 5(2) of the *FOIP Act* states that, if a provision of the *FOIP Act* is inconsistent or in conflict with a provision of another enactment, the *FOIP Act* prevails unless another Act or the FOIP Regulation expressly provides that the other enactment prevails despite the *FOIP Act*.

This provision is particularly significant for archives because most of the legislation prohibiting disclosure of information that is paramount over the *FOIP Act* does not set time limits on the prohibition. For example, there are no time limits on the prohibitions on disclosure in the paramount sections of the *Alcohol and Drug Abuse Act*, the *Child Welfare Act* or the *Maintenance Enforcement Act*.

Public bodies transferring records to archives should identify any records that are subject to any restriction or prohibition on disclosure under legislation that is paramount over the *FOIP Act* and any time limits that apply.

If another Act or regulation is paramount over the *FOIP Act*, information referred to in that Act or regulation may not be available for research (see Chapter 4.2 of this publication for further information).

Disclosure of Information by the Provincial Archives of Alberta or the Archives of a Public Body

The Provincial Archives of Alberta and the archives of public bodies may disclose information for research purposes subject to certain conditions.

The role of the Provincial Archives and other public body archives is to select, preserve and make available the non-current records of public bodies that have been preserved because of their enduring value. This includes legal, evidential, financial, and historical value.

For research purposes means for the purposes of a systematic investigation or study of materials or sources in order to establish facts or to verify theories. *Research* includes general historical and genealogical research.

The *archives of a public body* means an agency, other than the Provincial Archives of Alberta, that is authorized to perform archival functions on behalf of that public body.

The archives of a public body may be:

- a public body's own archives, in which case the records will remain in the custody or under the control of that public body (e.g., the archives of most post-secondary institutions); or
- the archives of another public body, to which records may be transferred under **section 3(e),** in which case the records will normally be in the custody and under the control of the archives; or
- an archival facility that operates under a contract or agency relationship with the public body, in which case custody may be transferred but control must be retained.

***Disclosure of personal information* (section 41(1)(a)):** This provision supplements **section 38(1)**, which also allows for the disclosure of personal information without a FOIP request.

If personal information is *less than 25 years old*, archives may not disclose it under **section 41(1)(a)**. The archives must either apply a relevant provision in **section 38(1)** to respond to a request or ask the requester to submit a FOIP request.

If the personal information requested is *25 or more years old*, the archives may disclose the information under **section 41(1)(a) (i)** if the disclosure:

- would not be an unreasonable invasion of privacy under **section 16**; or
- is in accordance with **section 40**, which specifies conditions for disclosure of personal information for a research purpose.

The information must not be disclosed if another Act or regulation that is paramount over the *FOIP Act* prohibits the disclosure.

Chapter 4.4 sets out guidelines for applying **section 16**.

If the personal information is about an individual who has been dead for 25 years or more, and satisfactory proof of that fact is provided, disclosure would not be an unreasonable invasion of privacy under **section 16(2)(i)** and the personal information may be disclosed under either **section 41(1)(a) (i)(A)** or **section 38(1)(a.1)**.

If the researcher cannot prove that the individual has been dead for at least 25 years, and it is determined, after application of the other provisions of **section 16**, that the disclosure would be an unreasonable invasion of a third party's privacy, the archives can only disclose the information in accordance with **section 40**, which requires a research agreement.

Information about research agreements and the application of **section 40** is provided in section 7.10 of this chapter. If disclosure is made under **section 40**, the archives must have a written agreement in accordance with **section 8** of the FOIP Regulation.

If the personal information is in a record that is *75 or more years old*, the archives may disclose that information subject only to the restrictions of any legislation that is paramount over the *FOIP Act*.

***Disclosure of information other than personal information* (section 41(1)(b)):** This provision allows for the disclosure of information, other than personal information, which is 25 or more years old. It supplements **section 83**, which allows the heads of public bodies to specify certain categories of information that may be made available to the public without a FOIP request.

Section 41(1)(b) is intended to establish greater transparency for archives, which tend to hold large volumes of records collected by public bodies. This transparency benefits not only public bodies that transfer the custody and control of their records to archives, but also the researchers who use the collections.

Section 41(1)(b) requires the Provincial Archives or the archives of a public body to assess the information and determine whether disclosure could still result in harm or whether disclosure may be prohibited for some other reason.

Information may be disclosed under this provision if:

- disclosure would not harm the business interests of a third party within the meaning of **section 15**;
- disclosure would not harm a law enforcement matter within the meaning of **section 19;**
- the information is not subject to any type of legal privilege under **section 26**; *and*
- access to the information is not restricted or prohibited by another Act of Alberta or Canada.

Details on the application of **section 15** are provided in Chapter 4.3 of this publication. If the information is in a record that has been in existence for 50 years or more, then **section 15** does not apply.

Details on the application of **section 19** are provided in Chapter 4.7 of this publication.

Details on the application of **section 26** are provided in Chapter 4.14 of this publication.

When public bodies transfer records to archives, they should identify any records that may be subject to restrictions imposed by other Acts. They should also identify any records to which the exceptions in the *FOIP Act* for disclosure harmful to the business interests of a third party or

harmful to law enforcement may apply, as well as any records that may be subject to legal privilege.

Accepted archival practice involves the accessioning of records according to organizational principles and standards that assist researchers in using the records. Archives may find it helpful to have policies in place that explain the relationship between their procedures and practices and the provisions of the *FOIP Act*. For example, if it is decided to apply **section 41(1)** to open a particular collection in the archives, the policy may set out the criteria that are used to determine that information in the record series meets the test of being 25 or more years old.

Archives of Post-Secondary Educational Bodies

Section 41(2) applies to the archives of post-secondary educational bodies. This provision supplements **section 41(1)** by allowing disclosure that would not normally be permitted. **The archives of post-secondary educational bodies may apply either section 41(1) or section 41(2) to disclose information.**

Section 41(2) permits a post-secondary educational body to disclose information from its archives for research purposes, if it enters into a written agreement with the researcher and if access to the information is not restricted or prohibited by another Act of Alberta or Canada.

This provision applies to all information in the archival records of post-secondary educational bodies, including personal information, if the information is at least 25 years old.

Information must not be disclosed if another Act or regulation that is paramount over the *FOIP Act* prohibits the disclosure.

Section 41(2) allows post-secondary educational bodies this additional flexibility to disclose information on the condition that the researcher enters into a written agreement. The agreement must:

- ensure security and confidentiality of the information, and
- prohibit subsequent use or disclosure of any personal information in individually identifiable form without express authorization of the post-secondary educational body.

For details on research agreements, see section 7.10 of this chapter.

7.12 RECORD OF PURPOSES

The *Act* requires that public bodies maintain a record of the purposes for which personal information in their personal information banks is disclosed, including all purposes that are deemed to be consistent with the purposes for which the personal information was originally collected (section 82(3)).

In order to meet this requirement, the public body must:

- retain a record of the purpose for which personal information in a record has been disclosed, and either attach or link that record to the personal information; and
- ensure that the purpose is included in the description of the relevant

personal information bank held by the public body.

There are a number of ways to meet the requirement to attach or link a record of purpose to the personal information. For paper files, when the request is for information about one or more individuals, a copy of the official request for use or disclosure of the personal information, together with the signature of the official or employee agreeing to such use or disclosure, can be attached to individual files. When the request is for a large number of files, a control file can be created, containing the same information.

If an individual whose information is contained in the file series requests his or her personal information, the part of the control file containing information about the individual must be considered for disclosure along with the other personal information.

If the use or disclosure involves computer files, a tag or other indicator should be inserted in the system linking the user to information regarding the request for and decision to allow the use or disclosure. The requirement to consider the disclosure of information in a control file applies in this case as well.

The maintenance of a record of purposes is an administrative procedure that should be restricted to exceptional uses or disclosures.

Public bodies should regularly review their descriptions of personal information banks in the directories of personal information banks they are required to maintain.

Public bodies should ensure that all uses and disclosures of personal information that are routine in nature and occur frequently are described in generic terms in the description for the appropriate personal information bank. This fulfils the requirement set out in **section 82** to notify the public about such uses and disclosures.

7.13 EXERCISE OF INDIVIDUAL RIGHTS BY OTHER PERSONS

Section 79 of the *Act* provides that another individual, under specific circumstances, may exercise any right or power under the *Act* that is conferred on an individual.

***Deceased individual* (section 79(1)(a)):** If an individual is deceased, the individual's representative or executor can exercise rights and powers under the *Act*. This exercise of rights and powers is limited to information relating to the administration of the individual's estate.

Proof of the right to act is normally a copy of the signed and attested document naming the representative to act in matters related to the estate. Evidence consisting of an applicant's stated belief in his or her authority, whether by affidavit or otherwise, or evidence that an applicant administered an estate is not sufficient (see *IPC Order 98-004*).

For information related to disclosure to relatives of deceased persons see Chapter 4.4 and section 7.8 of this chapter.

Guardian or trustee **(section 79(1)(b)):** If a guardian or trustee has been appointed for the individual under the *Dependent Adults Act,* the exercise of rights can be undertaken by the guardian or trustee. The rights or powers must relate to the powers and duties of the guardian.

The document governing the nature of the guardianship or trusteeship provides the authority for the representative to act. Public bodies should examine that document to ensure that the disclosure relates to the powers and duties stipulated in the document.

Personal directive **(section 79(1)(b.1)):** If an agent has been designated under the *Personal Directives Act*, the agent can exercise the individual's rights. The disclosure is limited to the powers given to the agent under the personal directive. Personal directives cannot provide authority over financial matters. Public bodies should examine the directive before disclosure.

Power of attorney **(section 79(1)(c)):** A power of attorney is an authority given to one person (called the attorney) to do certain acts in the name of, and personally representing, the person granting the power (called the donor).

A power of attorney can be to perform specific acts on behalf of the donor (the person who gives the power of attorney) or can be a general power of attorney to do everything that the donor can do. Donors can revoke some powers of attorney; some are irrevocable. Powers of attorney come into effect in the event of mental incapacity or remain in effect notwithstanding the mental incapacity of the donor, provided they comply with the provisions of the *Powers of Attorney Act*. The death of a donor normally revokes the power of attorney.

Public bodies should verify the identity of the person holding the power of attorney and ensure that the power of attorney allows for the disclosure requested or any other power or right being invoked.

It may also be necessary, depending on the nature of the power of attorney, to verify that the donor is alive or that the donor is not suffering from a mental incapacity.

Minors **(section 79(1)(d)):** If the individual is a minor, a guardian of the minor may exercise any right or power under the *Act*. This provision does not create an unlimited right of access on the part of a parent or guardian. **Section 79(1)(d)** is discretionary, and disclosure may be limited to circumstances where, in the opinion of the head of the public body concerned, the exercise of the right or power by the guardian would not constitute an unreasonable invasion of the personal privacy of the minor.

Records should be carefully reviewed in any situation where the information may be sensitive.

A *guardian* is a person who has care and custody of the minor or is involved in his or her daily care. This definition may not extend to the parents of a child in all circumstances.

Public bodies should have policies for dealing with minors based on the statutes and regulations under which they operate. When seeking decisions from individuals under the age of majority, public bodies should take into consideration their own policies and procedures for deciding when these individuals have the ability to understand the matter being decided and to appreciate the consequences of such a decision. The opinions and views of the minor constitute just one of the factors that must be taken into account in making a decision.

For information on the interpretation of **section 16** and the tests used to determine whether a disclosure would be an unreasonable invasion of privacy, see Chapter 4.4 of this publication.

***Written authorization* (section 79(1)(e)):** Any individual can provide written authorization to another person to act on his or her behalf. This authorization must be in writing, should generally provide authority to the representative to exercise any right or undertake any power, including the right to provide consent under various provisions of the *Act*, and be signed by the individual, preferably with an attestation by a witness.

An example of an **Authorization of Representative Form** is included in Appendix 6 of this publication.

Notices

Section 79(2) provides that any notice required to be given to an individual under the *Act* may be given to the person entitled to exercise the individual's rights and powers as provided in **section 79(1)**.

Chapter 8
Records and Information Management

8.1 OVERVIEW

The operations of public bodies involve the management of records and information for reasons that are significantly broader than the requirements of the *FOIP Act*. Organizations create, maintain and manage recorded information to provide tangible evidence of business activities and transactions.

Records and information management is generally carried out to:

- support policy formation and managerial decision-making;
- improve client services and support better performance of business activities;
- support consistency, continuity and productivity in operations, administration and management;
- protect the interests of the organization and the rights of clients, the public and employees;
- provide protection and support in litigation, including the better management of risks associated with the existence or lack of evidence of activities or events;
- facilitate research and development activities; and
- enable the organization to meet legislative and regulatory requirements.

To meet their obligations under the *FOIP Act*, public bodies need to have in place effective records and information management practices. This chapter is intended to help public bodies understand how these practices assist in the effective administration of the *FOIP Act*.

8.2 SCOPE

Alberta Innovation and Science has the statutory authority for the administration of a records management program in government. Alberta Government departments, boards and agencies subject to the Records Management Regulation (AR 57/95) must adhere to the policies and guidelines established under this Regulation.

For provincial public bodies, this chapter supplements the policies and guidelines issued by that department.

More detailed information on records and information management practices may be obtained from the *Records Scheduling and Disposition in the Government of Alberta* publication produced by Alberta Innovation and Science.

Local public bodies are not subject to the Records Management Regulation. Under **section 3(e)(ii)** of the *FOIP Act*, regulation of records management in local public bodies must be by by-law, resolution or other legal instrument by which a local public body acts, or, in the absence of such a legal instrument, as authorized by the governing body of the local public body.

Records scheduling and disposition in local public bodies should be based on recognition of the role of records management in effective public administration. In particular, local public bodies should be aware of the importance of an authorization process for the disposition of records that ensures that the local public body can meet its financial and legal obligations, including its obligations under the *FOIP Act*.

8.3 POWERS OF THE COMMISSIONER

Section 51(1)(a) of the *Act* authorizes the Commissioner to monitor the general administration of the *Act* to ensure that its purposes are achieved. This includes conducting investigations to ensure compliance with rules relating to the destruction of records set out in:

- any other enactment of Alberta;
- a by-law, resolution or other legal instrument by which a local public body acts; or
- any rules relating to the destruction of records that are authorized by the governing body of a local public body.

Public bodies, therefore, should expect their records and information management practices to be under scrutiny during reviews, investigations and privacy audits conducted by the Commissioner's office. This is especially the case when an applicant requests a review of the adequacy of a search for information or records.

8.4 RECORDS ISSUES RELATING TO ACCESS REQUESTS

The right of access to records which is provided in the *FOIP Act* is intended to make public bodies more open and accountable to the public. Inadequate record keeping can contribute to poor accountability to clients and the general public.

In the case of FOIP requests, a public body may find that poor records management can cause it to violate the *Act*. This may lead to:

- the credibility and reputation of the public body being challenged;
- costly use of resources to defend past actions rather than the use of resources to facilitate business processes in a proactive way; and
- the public body being exposed as negligent or ineffective in the discharge of its responsibilities through orders and reports of the Information and Privacy Commissioner and commentary from applicants, the media and interested members of the public.

Some common issues are outlined below.

Ability to Find Records

The access provisions of the *FOIP Act* assume an ability on the part of public bodies to identify, locate and produce records in response to requests. This ability is crucial both in making information routinely available to the public and in responding to FOIP requests.

The search process is greatly facilitated if a retrieval system is in place that allows staff processing an access request to search for a particular topic or subject and find all locations where records may be found.

The failure to capture records in effective record-keeping systems is the most commonly cited problem associated with inadequate management of records and information. (See, for example, *IPC Order 97-019* and *IPC Investigation Report 98-IR-009*.)

This may result in difficult and time-consuming searches for records, as well as uncertainty that all records relevant to a FOIP request have been located. This is particularly an issue when no records can be found on a subject, although it appears that a public body should have created and maintained a record on the subject and there is no evidence that the record was destroyed in an authorized manner.

An effective records management system should allow retrieval of semi-active as well as active holdings (*see IPC Order 96-021*). It should also allow retrieval of records in a storage facility, such as the Alberta Records Centre (for provincial public bodies).

In addition, the records management system should provide some ability to alert an applicant to the fact that records may have been transferred to the public body's archives (see *IPC Order 96-022*).

Applicants frequently challenge the adequacy of a search for records by a public body. Public bodies will find it easier to demonstrate thoroughness if there is an established record-keeping system. For an example of the analysis of a public body's record-keeping system and its search for apparently missing records, see *IPC Order 98-003*.

Public bodies also need to be able to show that the search has been conducted in a systematic and reasonable manner. The Commissioner has ruled that a limited "keyword" search does not constitute an adequate search (see *IPC Order 99-002*) and that public bodies should be able to locate all records that are "reasonably related" to the applicant's request.

The Commissioner has also stated that a search that relies on the memory of an employee is not in compliance with the *Act* (see *IPC Order 99-021*).

Standard of Documentation

A public body should have a standard of documentation. This requires clear direction from senior management as to how officials and employees will document business activities of the public body.

Employees should be held accountable for documenting their activities or transactions.

As well, there is a need in the modern electronic work environment to ensure that information technology systems have version control capability so that public bodies can retrieve the authoritative versions of documents.

Establishing standards will also address the issue of records that have been created but that are inadequate from the perspective of accountability. This may be because they are not completed accurately, or because it is impossible to determine the authoritative version of a record on which a decision or other action was based.

There is also need for clear direction on what records the public body considers are transitory in nature. For example, it may be decided that rough notes, messages, and routine office documentation, which have only short-term value, may be disposed of regularly at the discretion of an official or employee.

In the absence of such direction on transitory records, the Commissioner may require a public body to produce other evidence at an inquiry that a record that has been destroyed was appropriately destroyed as a transitory record (see *IPC Order 99-009*).

Transitory records are discussed in greater detail in section 8.6 of this chapter.

Finally, standards of documentation should clearly indicate that the official records of the organization cannot be altered or destroyed without authorization.

Alteration or destruction of records is a very serious matter, especially when done to evade a FOIP request, and could lead to penalties or sanctions. See Chapter 2.4 of this publication for information on the offence provisions of the *Act*.

Controls over Disposition

Cost-effective business practices dictate that a public body has a systematic process for disposing of records as they become inactive and are no longer needed for business purposes or the long-term operations of the organization (e.g., to protect the organization's interests in the event of litigation).

This process, known as records scheduling and disposition, has several advantages from a FOIP perspective.

First, it provides control over the disposal or destruction of records, so that public bodies know what was destroyed, and when. It also sets out what records of enduring value are transferred to archives. Establishment of records retention and disposition schedules – and compliance with them – allows public bodies to set accurate limits to searches for records.

Second, a schedule provides an official approval process for the disposition of records, including the destruction of transitory records, based on business needs. It provides evidence for the applicant, and for the Commissioner if necessary, that records have been appropriately disposed of by the public body.

The Commissioner has emphasized the importance of rules relating to the destruction of records, and he has noted that it is within the purview of the Commissioner to ensure compliance with such rules (see *IPC Order 98-011*).

Finally, a schedule allows for the movement of records through the system. This reduces the need for public bodies to tie up resources in the maintenance of older records, which may be very labour-intensive to locate and handle.

Older records that are needed to record the activities of a public body, to protect its interests or to provide long-term corporate memory for the public body can be placed in the Provincial Archives of Alberta, the archives of a public body, or other archival facility, as appropriate.

See Chapter 7.8 for a discussion of disclosure of personal information to archives, including the ability to disclose information to an archival facility that is not a public body, but which has a contract or agency relationship with a public body.

FOIP requests can then be dealt with by these organizations, which are usually well oriented to dealing with requests for records.

In summary, the lack of a systematic records scheduling and disposition system can mean that:

- older records are retained far longer than needed;
- there is random destruction of records, which can be embarrassing for a public body or may expose it to risks of litigation;
- there is no official authority for the legitimate disposition of records that are of no further use, including transitory records;
- resources may be wasted looking for records that no longer exist; and
- materials that should be permanently preserved may be lost.

Ability to Routinely Disclose Records outside FOIP

A public body needs:

- to have effective control over the records and information which it creates and collects; and
- to be knowledgeable about such records and information.

This is required to make effective decisions about which records should either be released on a routine basis or actively disseminated to the public.

Routine disclosure and active dissemination are practices that contribute significantly to openness in public administration and better client service.

8.5 RECORDS AND INFORMATION MANAGEMENT PRINCIPLES

The following principles underpin the effective management of recorded information.

The Management of Information is Planned

An organization's business planning processes require both strategic and operational records and information management planning.

All Records are Included

Management practices should apply to all records as defined in the *FOIP Act*, including personal information and electronic records.

Electronic records include:

- electronic documents, such as word processed documents, e-mail, web pages, graphics, digital photographs, and scanned images; and
- electronic data, such as information stored in databases.

Electronic records include information in all media and in all locations. For example, electronic records may be stored on networks, local hard drives and portable hard drives, as well as in storage media such as floppy disks, CD-ROM disks, optical disks, and tape.

Information is an Important Resource of the Organization

An essential principle for the management of recorded information is that information is managed as a resource or asset of the whole organization and not as the property of individuals, branches or divisions.

A Life Cycle Management Approach is Adopted

Sound principles for the management of recorded information are based on the life cycle of information. Management activities within the life cycle encompass:

- the planning of information systems, including appropriate controls over the collection, creation or compilation of recorded information;
- the establishment of practices and procedures governing the organization, distribution, retrieval, use, accessibility, and transmission of the recorded information and for its storage, maintenance and protection;
- provision for routine disclosure and dissemination of such information, as appropriate; and
- the regulation of the disposition of all recorded information.

Accountability is Assigned

In the case of provincial public bodies, the Records Management Regulation assigns accountability for records management in the public body to the deputy head.

Given the close relationship between the *FOIP Act* and the effective management of recorded information, there should be a similar assignment of accountability for the management of recorded information in local public bodies.

8.6 RECORDS AND INFORMATION MANAGEMENT POLICY COMPONENTS

Policy and guidelines should govern the management of recorded information in a public body. These should be developed with the administration of the *FOIP Act* in mind and include appropriate references to freedom of information and protection of privacy requirements in policy statements as well as in procedures, practices and standards.

Beyond principles, certain basic requirements or policies should be set out relating to both the management of recorded information and the public body's responsibilities under the *FOIP Act*.

The following components should be included in policies for the management of recorded information.

Life Cycle Management

The policy should require the public body to plan, direct, organize and control recorded information throughout its life cycle, regardless of the form or medium in which the information is held.

Establishment and Maintenance of a Records System

Another component of a records and information management policy is for a public body to establish a records system. A *records system*, which may be computerized or manual, is an information system which captures, maintains and provides access to records over time.

A records system should be controlled by a current, comprehensive and structured identification or subject classification system. Such a classification system provides an effective means of organizing, locating and retrieving all recorded information in the custody or under the control of the public body.

The records system should serve as a locator system for all holdings of recorded information. It should also identify responsibility for particular information. In addition, it should support the application of privacy protection measures

Guide to Information Holdings

An important component of a records system is the records inventory or guide to information holdings, which provides descriptions of the records in the system.

The guide to information holdings is a critical tool for the overall management of recorded information. It should support access to information both internally and externally to the public body. It should also support the application of privacy protection measures.

The guide to information holdings may also serve as the basis for establishing records retention and disposition schedules.

In addition, it may provide the elements of the descriptions of records in the custody or under the control of provincial public bodies for inclusion in the directory of records required under the *Act*.

In the case of local public bodies, the guide to information holdings may provide the elements of the descriptions of their personal information banks ("PIBs"). Each local public body must make available for inspection and copying by the public a directory listing all of its PIBs (**section 82(6)**).

Creation and Generation of Records

The policy should establish effective controls over the creation, maintenance and use of recorded information in the conduct of the business of the organization, through the establishment of a documentation standard.

This standard should indicate what records need to be created and maintained. For example, records required for legal, fiscal, audit, administrative or operational purposes should be retained in a records system.

The standard of documentation should be understood and followed by officials and employees of the public body.

A Guide for Transitory Records

The policy may enable all employees to destroy transitory records. A *transitory record* is a record that does not have long-term value. Transitory records contain information that is not required to meet legal or financial obligations or to sustain administrative or operational functions, and has no historical value.

A full definition of transitory records that has been developed for provincial public bodies is provided in the *Records Scheduling and Disposition in the Government of Alberta*, Chapter 2-9, and *A Guide to Identifying and Disposing of Transitory Records*, produced by Alberta Innovation and Science.

Local public bodies may develop and approve their own definitions, but must be prepared to defend deviations from recognized standards before the Information and Privacy Commissioner.

Certain types of recorded information are generally managed as transitory records:

- information of short-term value (e.g., notes kept to prepare official minutes of a meeting);
- duplicate documents;
- draft documents and working materials that are used to create a master record or that do not document policy changes or changes in decisions;
- personal messages and announcements;
- e-mail that does not document a decision or transaction on behalf of the public body. Public bodies should have an internal e-mail policy that aids officials and employees in deciding when e-mail information should be retained in records systems; and
- voice-mail messages; however, as with any other oral communication, if it is considered necessary to document a decision or transaction recorded on voice-mail, a record of the message concerned may need to be retained.

Organization, Storage and Protection of Recorded Information

An information policy establishing a records system will provide a framework for the organization and storage of recorded information that facilitates the location and retrieval of the information. The policy should also address information security and the protection of personal information, both for business and FOIP purposes.

The public body should have standards in place relating to the organization, control, storage, and protection of recorded information, including electronic records.

Special Rules for the Organization and Management of Electronic Records

Electronic records are subject to the *FOIP Act* and should be managed as part of any program for the management of recorded information.

Ideally, in an electronic records system, processes should be in place to ensure that, where necessary:

- individual records are uniquely identified;
- contextual data, or "metadata," relating to the specific record or transaction is preserved (this may consist of, for example, date, subject, names of correspondents or participants);
- records can be authenticated;
- there is version control;
- records are classified and indexed for retrieval;
- there are access controls;
- there are controls over the alteration of records, including audit trails on use, as well as processes in place to permit the disposal of obsolete records under approved processes and schedules; and
- there are processes in place to permit the disposal of obsolete records under approved processes and schedules.

An electronic records system should address the effective management, retention and disposal of e-mail.

If there is not an adequate electronic record-keeping system, the policy should require records to be printed and managed as part of the record-keeping system applied to hard copy records.

Planning of Electronic Information Systems

The application of new information technology within public bodies often has an impact on existing record-keeping activities.

An information management policy may establish a process for introducing the records system requirements into the planning and design of electronic applications that will collect, create or generate information used by the public body.

There are two special needs of public bodies that require special information management standards and specifications. These should be considered in the design of electronic information systems.

The first is the need to support routine disclosure of information outside the *FOIP Act*. Recorded information should be managed to promote public access where this is appropriate. It may be desirable that electronic information systems include a public access component.

Public bodies should ensure that opportunities for routine access are considered in the design and functional specifications for new or modified electronic information systems. This will facilitate routine disclosure and active dissemination of information, where appropriate, after the system is implemented.

Second, privacy protection measures must be considered in the design and functional specifications for information systems that are used to collect, generate, manipulate, and disclose personal information.

The particular requirements for protection of privacy are discussed in Chapter 9 of this publication.

Scheduling and Disposition of Recorded Information

Control over the disposition of recorded information is an important aspect of records management that is critical to FOIP administration. When responding to a FOIP request, it is necessary to know whether records have been destroyed and if so, whether this has been done in an authorized manner.

It is equally important to dispose of personal information under conditions that protect the privacy rights of the individual.

A records retention and disposition schedule is a public body's legal authority on how long recorded information must be kept and how it is to be disposed of (i.e., by destruction or archival preservation).

Each public body should establish a scheduling process that governs the retention and final disposition of all the recorded information in its custody or under its control.

For public bodies subject to the Records Management Regulation, the Alberta Records Management Committee approves records retention and disposition schedules. The schedules provide authority to transfer records selected for archival preservation to the Provincial Archives of Alberta.

The scheduling process is discussed in the Alberta Innovation and Science publication *Records Scheduling and Disposition in the Government of Alberta*, Chapter 2-2.

For other public bodies, authority to approve the transfer or destruction of the public body's recorded information will derive from its governing body. A public body may have its own archives, or may select the archives of another public body or another archival facility to act for it.

Public bodies must pay strict attention to disposal processes for records. This is true for all recorded information, but particularly so for personal information. Disposal processes should be governed by established and well-understood procedures.

All too often, sensitive personal information intended for destruction is left in insecure conditions and may be exposed to unauthorized access and, possibly, use. Examples include disposal of documents containing personal information in garbage bags that have ripped open and disposal of personal information in a recycling container.

Used office and computer equipment poses a special risk. In one investigation by the Information and Privacy Commissioner, filing cabinets were found to have been moved to an auction centre with files containing personal information still inside. Computer hard drives have been similarly put up for auction with information still stored on them.

Pulping or shredding is the best way of disposing of paper and other hard copy media. This should be done in a facility that can ensure complete and secure destruction.

At a minimum, computer hard drives and diskettes need to be professionally wiped clean of data before they are disposed of or sold.

Provincial public bodies are required:

- **to have operable hard drives wiped of all data by the ministry in accordance with specified procedures prior to sending the computers to Surplus Sales in Alberta Infrastructure; and**
- **to remove and destroy the hard drives in all computers to be surplused outside the government, except for those to be reallocated to the Computers for Schools program.**

See the Alberta Innovation and Science *Policy for Maintaining Security of Government Data Stored on Electronic Data Storage Devices* (November 1999).

For public bodies subject to the Records Management Regulation, destruction of recorded information must take place in accordance with the records management policies and procedures established by the Government of Alberta. Alberta Infrastructure, Surplus Sales, offers services to these public bodies for the wiping clean of computer hard disks before their disposal.

Records Management in Contracting

For programs and services contracted by public bodies to other agencies, provision should be made in policy for all contracts to require the contractor to create records that meet the public body's requirements.

Contracts should also require the contractor to maintain records according to standards acceptable to the public body for as long as required, to dispose of the records according to standards acceptable to the public body, or to return records to the public body, as appropriate.

When activities requiring the collection or handling of personal information are contracted out, the contract should set out the privacy protection and security obligations assumed by the contractor (see Chapter 9 of this publication).

Conditions governing FOIP and records management as they relate to contracting are further explained in the publication *Freedom of Information and Protection of Privacy: Contract Manager's Guide*, produced by Information Management and Privacy, Alberta Municipal Affairs.

Chapter 9
Privacy and Information Management

9.1 OVERVIEW

Part 2 of the *FOIP Act* establishes controls over personal information in order to protect individual privacy. These are generally called *fair information practices* and are based on a life cycle approach to the management of personal information.

The life cycle covers the collection and compilation, completeness and accuracy, protection, use, disclosure, retention and disposition of personal information. These fair information practices apply at each stage of the life cycle from creation to active record, to inactive record and then to final disposition.

The controls over personal information are dealt with in detail in Chapter 7 of this publication. However, effective implementation of the privacy protection measures set out in **Part 2** of the *Act* requires public bodies to adopt the management practices for personal information outlined in this chapter.

This chapter provides guidelines to help public bodies:

- establish a methodology for addressing privacy protection and related security issues when planning and establishing functional specifications for new or modified personal information systems;
- review personal information systems and bring them into compliance with **Part 2** of the *Act*;
- review forms used in the collection of personal information to ensure that they meet the collection and notification requirements of the *FOIP Act*;
- establish a security policy that supports protection of privacy; and
- manage data sharing and data matching involving personal information.

Planning New and Modified Personal Information Systems

Privacy protection requirements set out in **Part 2** of the *FOIP Act* should be fully integrated into the design, construction and implementation of computerized information systems used to process personal information.

Public bodies collect and use a wide variety of personal information in order to carry out their programs and deliver services. Increasingly, computer and computer-related technology is used to provide faster, easier and more cost-effective ways of handling and storing this information and the records created from it.

Electronic databases help public bodies to streamline processes, improve services and constrain costs. Greater automation and integration of information and operational systems are often strongly encouraged by legislators and public servants alike as a vital part of making government more relevant, effective, affordable and geared to serving the needs of citizens.

At the same time, these applications of new technology may make individuals question whether their privacy is threatened and whether their personal information may be put to uses that they never intended.

To ensure that privacy protection considerations, as set out in **Part 2** of the *FOIP Act*, are taken into account in the application of new technologies, public bodies may need to conduct a *Privacy Impact Assessment* or a *Security Impact Assessment* and to submit it to the Information and Privacy Commissioner for review.

A *Privacy Impact Assessment* requires a public body to look at how its activities, especially the application of technology, affect the privacy of individuals. A Privacy Impact Assessment involves consideration, during the planning and implementation of a program or system, of appropriate and effective measures to ensure compliance with **Part 2** of the *Act*.

Examples of initiatives that would be likely to need a Privacy Impact Assessment include:

- the creation or significant modification of databases containing personal information, particularly where the information is sensitive or includes a significant number of people;
- identification and authentication schemes, especially proposals for multi-purpose identifiers or those that make use of biometrics;
- schemes that might reduce or eliminate existing opportunities for anonymity through program or service channel redesign;
- the introduction of a "smart card."

The challenge for public bodies is to integrate privacy protection into technology systems development in ways that enhance information and data quality, integrity, accuracy, and confidentiality.

A *Security Impact Assessment* requires a public body to look at how personal information will be protected from unauthorized access, use and disclosure.

Privacy and security measures should not be viewed as barriers to applying innovative technology. Rather, they are essential components of modern systems that serve to build public confidence in the use of technology. In the last decade, a number of technologies have been specifically developed to be *privacy-enhancing technologies*.

Technologies such as encryption, digital signatures, anonymous electronic cash and service delivery systems, and "pseudo-identification" can often enhance privacy at little or no extra cost. They may also have the advantage of providing more secure identification to reduce fraud, more secure networking to reduce losses from theft, and more secure payment systems to eliminate the administrative costs of cash transactions.

Privacy-enhancing technologies make it clear that cost savings and privacy protection need not be opposing values. Quality management of technology should go hand in hand with privacy protection.

Public bodies should establish practices and procedures that take into consideration the requirements of

Part 2 of the *Act* in the planning, design, development of specifications, and implementation of information technology for new or modified personal information systems.

9.2 PRIVACY AND SECURITY IMPACT ASSESSMENTS

In order to integrate privacy and related security considerations into the design, construction and implementation of new computer information systems that are used to process personal information, public bodies should take the following steps.

- Systems development should take into consideration the privacy rights of individuals and the protection of personal information. This applies to all aspects of the management of information, including collection or compilation, controls on accuracy, use and disclosure, protection, and disposal. Privacy considerations should be integrated at the earliest stages of development of automated information systems to ensure that such systems reflect legal and policy requirements.

- Whenever a computer-based system involving personal information is being developed or substantially modified, public bodies should ensure that the program official responsible for the project develops a Privacy Impact Assessment and a Security Impact Assessment as part of the business needs analysis or project initiation stage of the project.

- The project team for information systems projects dealing with personal information should include the FOIP Coordinator, the Senior Records Officer or senior records management staff, and senior personnel responsible for security and information technology security.

- Public bodies should ensure that the business analysis, project initiation or other type of basic project approval report contains the Privacy Impact Assessment and the Security Impact Assessment. It should be shared with the Office of the Information and Privacy Commissioner, with a request for comments on the project and the privacy and related security approaches being planned.

  A reply should be requested from the Commissioner's Office in a reasonable time period (e.g., 30 days). Any comments from the Office of the Information and Privacy Commissioner should be considered before senior officials in the public body approve the initiation of the project.

- More detailed privacy and related security specifications should be developed as the project moves to the feasibility stage. These should incorporate, as far as possible, the comments from the Office of the Information and Privacy Commissioner.

  These specifications should form an important element of the criteria on which senior management base their review of alternative solutions and the selection of a technological approach.

- Any public announcement concerning the new project should include a reference to the Privacy Impact Assessment and offer such information to the public upon request. For security reasons, it may not be possible to disclose the Security Impact Assessment.

- Any cost–benefit analysis of the system or application prepared at the feasibility stage should include a section on privacy implications. The analysis should not just set the least costly solution against the additional costs for privacy protection, but also examine the best value for money. The cost–benefit analysis should reflect good privacy solutions and enhanced public confidence as primary objectives for the system or application.

- Any report prepared at the feasibility stage should be shared with the Office of the Information and Privacy Commissioner to assure everyone that privacy and related security issues are being addressed in a satisfactory manner.

  Later in the process, at the design stage, the Office of the Information and Privacy Commissioner should also be sent a summary of functional specifications and the final draft description of the entire system or application. This provides a last opportunity for comment before embarking on the final design stage.

  Public bodies should be aware that Privacy Impact Assessments that are submitted to the Commissioner are considered public documents. Public bodies should make sure to identify any portions relating to security that should not be publicly disclosed.

- The privacy protections that have been built into the new system should be communicated to citizens, clients and employees. Public bodies should ensure, as the system or application becomes operational, that everyone is aware of the client's privacy rights and the public body's obligation to respect them.

- The first internal audit or review involving the system should include a section on privacy and protection of personal information, as well as related security issues, in order to determine whether the stated system design objectives in these areas are being met.

Privacy Impact Assessment

A *Privacy Impact Assessment* should include:

- A description of the project and of the nature and sensitivity of the personal information involved;

- A discussion of the relevant privacy principles and potential issues for the project, as well as suggestions as to how they should be addressed. Attention should be paid to how the system can improve privacy. Solutions to privacy issues should always focus on limiting access by employees to only that information needed to accomplish program objectives;

- A data flow analysis, including a description of the uses of the personal information and all consistent purposes and authorized disclosures that can be foreseen and may be sanctioned under the system. Any potential data sharing, data matching, front-end verification procedures and data linking should be identified;

- Consideration of how the privacy requirements in **Part 2** of the *FOIP Act* will be met. Collection and compilation of data, notification of individuals, use, disclosure, access, correction, protection, retention, and disposition of personal information should all be addressed; and

- An overall assessment of the privacy impact as high, medium or low, and an analysis of threats and risks. An assessment might include some consideration of public expectations and offer a general recommendation to decision-makers as to which potential solutions best address the combination of business needs and privacy principles and obligations, as well as allowing for the effective application of technology.

If the Privacy Impact Assessment relates to an initiative that involves the flow of personal information across jurisdictions, the public body should consider the implications of this for the protection of personal information. Particular attention should be given to determining whether the *FOIP Act* or other privacy legislation will apply to the personal information.

Public bodies planning to submit a Privacy Impact Assessment to the Information and Privacy Commissioner may find it helpful to seek further information or advice from the Office of the Commissioner before beginning the process. The Office of the Information and Privacy Commissioner has produced a short guide entitled *Suggested Elements for a Privacy Impact Assessment*.

Security Impact Assessment

A *Security Impact Assessment* should include:

- A statement of sensitivity for the personal information involved. This is drawn from the Privacy Impact Assessment;

- A statement of the business operation being developed, with a description (e.g., administration of a benefit program) and an initial assessment of expected standards for information and data integrity, quality, accuracy, availability, and confidentiality;

- The location and distribution of the information. This includes office locations, mainframe or distributed network, and whether the information is all electronic or a combination of electronic, hard copy and other formats;

- An analysis of potential threats to the personal information as a result of, for example, unauthorized access or disclosure, or modification or destruction of the information. The analysis should address administrative, physical and technical threats, whether accidental or deliberate, in relation to the risk of occurrence and the consequences that could result; and

- General recommendations for a security approach.

More detail on the development of security measures for personal information is provided later in this chapter.

When the development of personal information systems is contracted out, the need to develop Privacy Impact and Security Impact Assessments should be among the privacy requirements included in any management or operations contract governing the project.

9.3 CHECKLIST FOR THE REVIEW OF PERSONAL INFORMATION SYSTEMS

The collection, use, disclosure, and retention requirements of **Part 2,** Protection of Privacy, in the *FOIP Act* are very much oriented to information management practices. These provisions may require modifications to the information management practices of public bodies and to the operation of manual, automated and electronic information systems that are used to collect, compile, organize, manipulate, and retrieve personal information.

Public bodies should have policies and organizational structures in place that will facilitate the integration of privacy protection requirements and practices into the ongoing management of personal information systems.

A plan to bring any non-complying program activities and personal information systems into compliance with Part 2 of the *FOIP Act* should also be in place.

This section provides a checklist to help public bodies review their personal information systems and bring them into compliance with **Part 2** of the *Act*.

It is divided into *mandatory* and *optional* provisions. The mandatory provisions are required under the *Act*. The optional provisions are good management practices that should be considered but are not required.

Part 2 of the *Act* and Chapter 7 of this publication should be carefully studied while using this checklist.

The checklist can be used in relation to both automated and manual information systems.

Bringing information systems into compliance with the privacy provisions of the *Act* will assist public bodies in:

- supporting the public right to know what personal information public bodies collect and how this information is used;
- supporting the right of individuals to access their own personal information;
- assuring individuals that their personal information is protected from unauthorized collection, use and disclosure;
- ensuring public confidence in such systems and the programs which they support in terms of how personal information is handled;

- contributing to the highest quality of management and effectiveness for such systems, especially electronic systems; and
- establishing additional accountability for the protection of individuals' right of privacy by improving the management of personal information.

Collection of Personal Information: Authorization for Collection (section 32)

Section 32 limits the personal information that may be collected by public bodies. Collection must be authorized under **section 32(a), (b)** or **(c)**.

Mandatory

- Does an enactment of Alberta or Canada specifically authorize collection of the information?
- Is the information collected for the purposes of law enforcement? *or*
- Does the information relate directly to and is it necessary for an operating program or activity of the public body?

At least one response must be *yes*. If none of the above statements elicits a *yes* response, a review of the collection is required to determine whether it is still needed by the public body and, if so, how the collection may be brought into compliance with the *FOIP Act*.

Optional

- Is there a collection control and approval mechanism in place to ensure that the minimum amount of personal information necessary to carry out a program or activity is collected?

If the answer is *no*, consideration should be given to establishing such a control and approval mechanism.

Collection of Personal Information: Manner of Collection (section 33(1))

Section 33(1) requires a public body to collect information directly from the individual the information is about except in certain limited circumstances.

Mandatory

- Is the personal information in the system collected directly from the individual the information is about (direct collection)?

The answer must be *yes*, unless the public body is authorized to collect information indirectly.

- If the personal information in the system is collected from a source *other than the individual the information is about* (indirect collection), is there authority in **section 33(1)(a) to (k)** for indirect collection?

If there is no authority in **section 33(1)(a) to (k)**, a revision of procedures or of the collection itself is required. This may mean collecting the information directly from the individual, seeking his or her consent for indirect collection of the information or ceasing the collection. The only exception to this would be if **section 33(3)** applies.

Optional

- Is the authority for collection described in the documentation for the system?

Collection of Personal Information: Notification of Collection (section 33(2))

When personal information is collected directly from an individual, notification of the purposes and authority for the collection must be provided to the individual.

Mandatory

- If information is collected directly, does the notification provided to the person from whom the information is collected include:
  - the specific purposes for which the information will be used?
  - the specific legal authority for the collection of information? *and*
  - the title, business address and telephone number of an official in the public body who can answer questions about the collection of personal information?

The answer must be *yes* on all three requirements set out in the *Act*. If the answer is no, modifications may be needed to the processes of notification.

- If notification is *not given* to the person from whom the information is collected,
  - does one of the paragraphs in **section 33(1)(a) to (k)** apply? *or*
  - has the head of a public body excused the need for notification because compliance would result in the collection of inaccurate information?

If neither of these questions can be answered with a *yes*, a revision of collection procedures or the type of information collected is required.

- Is the method of notification appropriate?

Examples of different methods of notification include notice on a form or in a pamphlet or other publication, oral notice, a pop-up screen on a computer terminal, a card or notice on a desk or counter, and a voice-mail message.

Optional

- Is a copy of the notification of collection and use given to the person from whom the information is collected?

- Is a copy of the notification also kept on file by the public body?

- Does the notification of collection and use include notice of:
  - the right of the person the information is about to request a correction?
  - the right of the person the information is about to appeal a refusal to correct information? and
  - a description of the role of the Information and Privacy Commissioner?

- If personal information in the system is collected from a source *other than the person the information is about* (indirect collection):
  - is notification of collection provided to the person the information is about?
  - in cases where personal information is downloaded from another public body's system rather than input directly, is the individual the information is about informed of this data sharing when the other public body collects the information?
- If the information is collected on an electronic form, through a touch-tone telephone, or by keying it directly into a database during an interview,
  - is there provision for obtaining the individual's signature or other verification of identity?
  - is a hard copy of the completed form or a printout from the database provided to the person from whom the information is collected?
  - is a hard copy notification of collection provided to the person from whom the information is collected, if applicable?
  - does the office retain a copy of any documentation relating to the collection?
- Do these or other measures provide some form of audit trail of the source of the information and the notification of collection and use, if applicable?

Accuracy of Information (sections 34(a) and 35)

A public body must make every reasonable effort to ensure that personal information used to make decisions that affect an individual is accurate and complete.

Mandatory

- Can it be determined when the record containing personal information was last updated?
- Is a record kept of the source on which the change was based, either through a hard copy or an automatic logging of transactions so that it is possible to recreate any addition, deletion or modification of information?
- Are procedures in place to ensure that individuals can review their own personal information and request correction or annotation in case of errors or omissions?
- Are procedures in place so that, if necessary, notification of a correction or annotation of personal information can be sent to any other public body or third party to which the information has been disclosed during a one-year period prior to the correction or annotation?
- Is a record kept of all updates to files, including requests for correction or annotation?
- Is there a system of verification for personal information collected and for its entry on the system?
- Are recovery routines and procedures in place?
- When changes of system technology are required, are procedures documented and implemented to

ensure the integrity of the operating system and supporting software?

- In electronic systems, are computerized records compared at appropriate intervals to an independent source as a basis for verifying the accuracy and completeness of stored data?
- Are there adequate validation procedures to automatically identify and correct errors and omissions?
- Does a responsible authority review these actions and procedures?

If the response to the above questions is generally *no*, then a revision to system procedures is required.

Retention of Personal Information (section 34(b))

Section 34(b) requires retention of personal information used to make a decision about an individual for one year in most cases.

Mandatory

- If information has been used to make a decision that directly affects an individual, are procedures in place to ensure that the information is retained for at least one year after use?

If the answer to this question is *no*, the public body needs to establish a procedure to ensure compliance with the *Act*. This will require flagging any record of personal information used to make a decision about an individual and retaining it for a year after each decision. If a records retention and disposition schedule is in effect, this requirement overrides any retention period based on the *date* of the record, since it relates to *use* of the record.

Optional

- Are records retention and disposition schedules in place for information in personal information banks that are in the custody or under the control of the public body?

If the response is *no*, the public body needs either to establish a records scheduling process or make a revision in current records scheduling procedures and practices to make specific provision for personal information banks.

Protection of Personal Information (section 36)

A public body must make reasonable security arrangements for the protection of personal information against such risks as unauthorized access, collection, use, disclosure, and destruction.

While the checklist deals with a whole range of security issues, the basic attributes for a comprehensive security policy and practices are provided in section 9.5 of this chapter.

Mandatory

Responses to the following should be proportionate to the sensitivity of the personal information in the system.

- Are all personal information sources identified?
- Does a security policy and procedure govern operations?
- Is there a responsible official who has authority for the security of the system?

- Are there documented procedures for collecting, processing, accessing, transmitting, storing, and disposing of personal information?
- Do security procedures cover administrative, physical and information technology security, including:

  - a threat and risk management methodology?
  - a process for designating sensitive information and assets?
  - a system of authorization and access procedures, such as the use of identification cards and the maintenance of control records for gaining access to sensitive personal information and for gaining access to sensitive material and items, such as keys, codes, combinations, badges and system passwords?
  - controls over authorization to add, change and delete personal information in a system, and transaction controls to determine when personal information in a system was last updated, who updated it and who has accessed it?
  - procedures to ensure that qualified personnel are involved in the maintenance of electronic systems in order to ensure configuration control of equipment, systems, networks, and the updating of operating procedures?
  - procedures for ensuring communications security and appropriate controls over cryptographic materials where this is required?
  - procedures for adequate reference checks and screening of personnel which are commensurate with the sensitivity of the personal information involved?
  - controls that restrict use of personal information to the purposes for which the information has been collected and restrict access to those officials and employees who have a "need to know" the information (i.e., access is limited to the specific portions of the personal information needed for the function being performed)?
  - appropriate physical security measures such as security access zones, locked rooms, storage cabinets, controlled positioning and access to computer terminals and faxes (to prevent random access), as well as checkout and secure transmission procedures for files? *and*
  - secure disposal procedures for records and equipment commensurate with the level of sensitivity of the personal information and its vulnerability to compromise?

- Is there any monitoring and review of the general effectiveness of security measures including those relating to the protection of personal information?

If the general response to the relevant requirements is *no*, it will be necessary to establish security policies and procedures for the personal information system or revise them.

Use (section 37)

Section 37 limits the purposes for which public bodies may use personal information.

Mandatory

- Is the personal information in the system used only:
  - for the purpose for which it was collected or for a use consistent with that purpose?
  - with the consent of the individual, in the prescribed manner? *or*
  - for a purpose for which information may be disclosed under **sections 38, 40** or **41** of the *Act*?

If none of these questions is answered *yes*, then the uses of the personal information in the system need to be examined, and activities that do not meet the above tests must be discontinued.

- Is the personal information used only to the extent necessary for the public body to carry out its purpose?

If the answer to this question is *no*, the use needs to be examined to determine how the amount of information used could be limited in a way that would still allow the public body to carry out its purpose in a reasonable manner.

Disclosure (section 38)

A public body may disclose personal information only in accordance with the provisions of **section 38**.

Mandatory

- Does any person or body outside the organizational unit that operates and uses the system have access to information in the system, either directly through electronic means or through receipt of hard copy, tapes, diskettes or other copies?

If the answer is *yes*, then access controls must be reviewed.

- Does the disclosure fall within one of the provisions of **section 38(1)(a) to (dd), section 38(1.1) or section 38(1.2)** of the *Act*?

If the answer is *no*, then the disclosures that do not meet the requirements of **section 38** must be discontinued.

- Is the personal information disclosed only to the extent necessary for the public body to carry out its purpose?

If the answer to this question is *no*, the disclosure needs to be examined to determine how the amount of information disclosed could be limited in a way that would still allow the public body to carry out its purpose in a reasonable manner.

Research or Statistical Purposes (section 40)

A public body may disclose personal information for a research purpose only under specified conditions.

Mandatory

- Is access to personal information in individually identifiable form necessary to reasonably accomplish

the purpose of the research, or has the Information and Privacy Commissioner approved the research purpose?
- Is it clear that any record linkage is not harmful to the individuals the information is about?
- Are the benefits of the record linkage clearly in the public interest?
- Has the researcher signed an agreement to comply with security and confidentiality conditions, to meet a schedule for the destruction of individual identifiers and to ensure that there is no subsequent use or disclosure of the information in individually identifiable form without express authorization?
- Does the agreement meet the requirements set out in the FOIP Regulation?

All of the above questions have to be answered *yes* in order for a disclosure to be made under **section 40**.

Data Sharing and Data Matching

Data sharing and data matching involve the disclosure, exchange or comparison of personal information for an authorized purpose. These activities may involve public bodies only or public bodies and other organizations. The data sharing or matching may occur through electronic or other forms of transmission and may consist of single transactions or programs that continue over a period of time. These activities are subject to the provisions of **Part 2** of the *FOIP Act*.

See section 9.6 of this chapter for definitions and a detailed discussion of data sharing and data matching.

Mandatory

- In any data sharing or data matching:
  - is there authority to collect the information under **section 32** and to collect information indirectly under **section 33**?
  - do the uses meet the requirements of **section 37**? *and*
  - do any disclosures meet the conditions in **section 38**?

If the answer is *no* to any of these questions, the system is not in compliance with **Part 2** of the *FOIP Act* and the public body must modify or discontinue the data sharing or data matching.

Optional

- Are individuals whose personal information may be the subject of data sharing or data matching notified of this at the time the information is collected?

Record of Purpose (section 82(4))

This provision applies only to provincial public bodies.

A record of purpose must be maintained for any use or disclosure of personal information, if the purpose is not included in the *Alberta Directory of Records*, and this must either be attached or linked to the personal information. Public bodies need to be able to provide information to the public on all their personal information banks, including accurate, current information on the purposes for which the personal information may be used or disclosed.

Mandatory

- Is there a process for identifying uses and disclosures and is a record being linked or attached to the personal information each time uses or disclosures take place?

- Is there provision to notify the Minister, through Information Management and Privacy, Alberta Municipal Affairs, of the purpose of any use or disclosure not included in the publicly available directory of records?

If the answer is *no* to either question, the personal information system is not in compliance with **section 82(4)** of the *Act*.

9.4 REVIEW OF FORMS

Section 33(2) of the *Act* requires that a person be notified of the purpose for which personal information is being collected from him or her, the legal authority for the collection, and the name of someone who can answer questions about the collection.

Forms are a major way of collecting personal information. For that reason, it is important to bring forms (paper and electronic) into compliance with the privacy protection provisions of the *FOIP Act*.

In doing so, public bodies will:

- support the right of individual citizens to know what personal information public bodies collect about them and how this information is used;
- support the right of individuals to access information about themselves; and
- help maintain confidence among individuals that public bodies are protecting their personal information from unauthorized collection, use and disclosure.

As indicated in Chapter 7 (sections 7.2 and 7.3) of this publication, achieving compliance with the collection requirements set out in **sections 32** and **33** of the *Act* requires a thorough review of a public body's collection activities. Included in this should be a review of all forms to ensure that those used to collect information directly from individuals meet the privacy requirements and that any unnecessary forms are eliminated.

This may be a process of some magnitude for public bodies that have a large amount of personal information in their custody or under their control. For that reason, the review process will likely be planned and implemented over time, often on a program or service basis.

Revisions should be considered when there is a need to reprint or redesign forms. There should also be a priority list of significant forms that need revision as soon as possible. This may be because of the sensitive nature or the volume of personal information collected on these forms, or the extent to which the particular forms are used.

Where necessary, public bodies should make interim arrangements to ensure that individuals receive the notification required under **section 33(2)** when personal information is collected directly from them. This may be done by printing supplementary sheets containing a privacy statement to go with the forms, or by producing a short brochure or bulletin that explains the privacy protection being offered by the particular program or public body. Computer-based forms can be updated with a privacy statement almost immediately.

To facilitate interim notification measures, public bodies may print a supply of notifications covering:

- the purpose for which the information is collected;
- the authorization for collection;
- the name and telephone number of a person who can answer questions about the collection.

These may be provided to clients or attached to the forms being provided to individuals.

In cases where some personal information on a form should no longer be collected, public bodies should inform staff and clients that certain fields must not be filled out. These instructions should be provided in writing, and staff should take steps to achieve consistency in their approach to handling forms. In some instances, it may be possible to black out fields that are no longer required.

A review of forms and other collection instruments may be combined with the review of personal information systems discussed in section 9.3 of this chapter.

Notification

The notification may be printed on the collection form itself, on a separate or covering document that explains the form and how to fill it out, or it may be given verbally. Oral notification is practical when information is taken personally over the telephone, given by touch-tone telephone or taken during an interview.

When the privacy statement is provided orally, care must be taken to provide the individual with a copy of the privacy statement either at the office where collection takes place or with the documentation sent to an individual to confirm collection of information over the telephone or electronically.

An example of notification is as follows:

This personal information is being collected under the authority of (state Act or program) and will be used to (state known purposes). It is protected by the privacy provisions of the Freedom of Information and Protection of Privacy Act. If you have any questions about the collection, contact (name, address, and business telephone number of responsible official or employee).

Optional Practices

There are a number of practices for the collection of personal information through forms that reflect good management of personal information but are not mandatory under the *FOIP Act*.

Examples of good practices include:

- notification of the authority for collection and the purposes for which personal information will be used on all forms used to collect personal information from the public, whether or not this is required by the *Act*;

- design of forms to ensure that the individual from whom the information is collected is given a copy of the notification;
- design of forms to ensure that a copy of the notification is also retained by the public body;
- detailed notifications where appropriate to inform the individual about his or her right to request correction of inaccurate or incomplete information, the right to appeal refusals of corrections and the role of the Information and Privacy Commissioner in reviewing such refusals;
- central review of all new forms and proposed revisions before finalization for printing, including review of privacy issues; and
- where personal information is collected from a source *other than the individual the information is about* (indirect collection), provisions to inform individuals generally that information about them is being sought from a variety of specific sources. Such explanations should be included in documentation or brochures given to individuals who are the subjects of the indirect collection.

Electronic Forms

There are a number of special factors that should be taken into consideration when dealing with computer-generated forms or when planning to move into an electronic forms environment:

- a policy and accountability structure should be put in place to ensure that privacy statements are included on electronic forms, which are often generated on a decentralized basis;
- when new forms software is under consideration, one of the specifications should be that it permits the easy addition of privacy statements in ways that are convenient and that effectively inform the individual filling out the electronic form of his or her privacy rights;
- provision should be made for authorization of indirect collection and for authorization of additional uses or disclosures of the information on electronic forms where this is appropriate, as well as for a signature or other verification of the identity of the individual providing the authorization;
- a hard copy of the form should be provided to the individual the information is about, including the notification of collection on the form; and
- the public body should be able to retain a copy of the authorization and notification.

These practices establish an audit trail within electronic information collection for the authorization of collection, the source of the information and the notification of collection and use. If these practices are not used, some other audit practices should be in place.

Review Process

The following practices can assist in bringing existing forms into compliance with the *Act*:

- since the revision of forms may be a significant task, establish a plan which stretches over several years for revision;
- concentrate first on those forms used to collect information directly from individuals and choose the most visible or most used forms in this category for early review and revision. Leave other changes that are optional and not mandatory under the *Act* until later;
- carefully review and refine the notification statement to be included on or attached to the form and integrate the statement into the design of the form;
- establish a process where new forms can be quickly reviewed to ensure they meet the privacy standard established by the public body;
- include the requirements of the *Act* in the normal forms review process;
- keep stocks of all forms used to collect personal information at minimum levels pending review; and
- make revisions to forms at normal reorder points to avoid special printing runs.

Interim measures may be set up pending forms revision:

- train staff that receive forms containing personal information over the counter on how to give a verbal notification that meets the requirements of the *Act* and provide statements indicating that the privacy provisions have been explained;
- prepare a supply of photocopied notifications covering the purpose for which the information is collected, the authorization for collection and the uses to which the information will be put, and provide these to clients or attach them to the forms being provided to individuals;
- establish and maintain an inventory of forms used for the direct collection of personal information and establish a monitoring function to detect forms that do not include the appropriate notification.

9.5 SECURITY POLICY AND PRACTICES

Section 36 of the *Act* requires a public body to protect personal information by making reasonable security against such risks as unauthorized access, collection, use, disclosure or destruction.

Reasonable security arrangements are usually practices and procedures expressed through a security policy approved for use within a public body. This policy should deal with physical, administrative and information technology security and be geared to a risk and threat analysis of the information and assets in the custody or under the control of a public body.

The basic attributes of a security policy that recognizes privacy protection requirements are set out below.

Attributes of a Comprehensive Security Policy

Many organizations have restricted security policies to one particular area, such as information classification, administrative security or information technology security. An approach to security by functional area begins to falter in the face of the more global challenge of protecting a class of information, such as personal information.

A more comprehensive approach to security administration, including all aspects of physical, administrative and information technology security, is both necessary and practical.

The sharing and use of personal information by a number of public bodies creates an additional challenge. The *Act* requires reasonable protective measures for such information, but this will now require more consistency among public bodies in how they handle and protect such information. Comparability in protective measures among public bodies doing public business with each other is essential.

***Authority*:** A security policy should contain a statement of the authority or authorities under which the security policy is being issued and a direction from the senior officer of the public body on its effective implementation.

***What needs to be safeguarded*:** All assets of a public body, including information, require good basic care. Some assets, however, are more sensitive or valuable and require additional safeguards.

A policy should include a requirement to carefully identify sensitive information, valuable assets and information systems that may need additional safeguards.

***Sensitive information*:** Certain information will be excepted from disclosure under the *FOIP Act* because it would reveal particular sensitive information or pose possible injury to public or private interests. These categories of information are generally described in the exception criteria of the *Act*. Public bodies should take greater care in protecting these categories of information than they would information that is generally available to the public.

Among these categories is personal information. The *Act* defines personal information in **section 1(1)(n)** and **section 16** provides guidance as to what is an unreasonable invasion of personal privacy. **Section 16** is considered in detail in Chapter 4.4 of this publication.

The categories in **section 16** help to identify sensitive personal information that may need safeguards. Health information, financial information, pay and benefits information, and criminal records are particularly sensitive and require additional protection.

***Information technology security*:** The security of computer and telecommunications equipment and systems requires special consideration. This is due in part to the need to protect sensitive information, such as certain categories of personal information. It is also due to the significant extent to which many public body operations and services are dependent on information technology.

In addition to protecting the confidentiality of the information in these systems, it is necessary to define the importance that accuracy, completeness and availability play in the management of the public body's information technology systems.

Defining the importance of the availability of information and services is the first step in making plans to resume business within acceptable time and resource limits in the event of loss of data, programs or systems.

Also important is the identification of potentially vulnerable communications systems. The risk of someone overhearing sensitive personal information on the telephone or through a data line should not be neglected given the ease of such access. Facsimile machines warrant special attention because of the chance of misdirecting sensitive information through an error in transmission and because they are generally accessible to anyone in an office area.

What safeguards are required?

The policy should require a risk and threat analysis for security. This should include identification of what potentially requires safeguards and an assessment of threats and risks to the information, assets and information systems. This analysis provides the basis for assigning safeguards at a level commensurate with the risk. The security measures can be monitored and adjusted over time.

The policy should:

- require program areas to maintain complete and up-to-date inventories of personal information and personal information systems;
- provide for the review of potential threats (e.g., how could sensitive personal information be lost or changed?, what impact would this have on client confidence in the programs?, who would be affected and how?); and
- require the application of administrative, physical and technical safeguards and a personnel security program.

Examples of administrative, physical and technical safeguards include:

- written staff responsibilities and security procedures;
- arrangements to resume operations in the case of loss of computer-based data or capabilities;
- use of physical barriers, security zones, access and authorization mechanisms, and locked containers to restrict access;
- use of proper containers and procedures for the secure processing, storage, transmission and disposal of information and other assets;
- use of software, hardware or operating system access controls; and
- use of secure communications and cryptography where the sensitivity of the personal information and the magnitude of risk warrant it.

***Personnel security*:** Personnel security involves a process of checking the references and background of an officer or employee to ensure that he or she is a suitable person to have access to sensitive information, information systems and the facilities where they are located.

Personnel security also enables implementation of the "need-to-know principle," where access to particular information or systems can be limited to certain officers and employees who have a need for such access because it is necessary to perform their duties.

A security policy should set out some type of personnel security process.

Breaches and Violations

A security policy should establish what are considered breaches and violations of security.

A *breach* is the breaking of a rule or promise, not necessarily intentionally. For instance, someone who is not thoroughly acquainted with the procedures for handling sensitive personal information may put it at risk.

A *violation* occurs when someone wilfully and knowingly breaks an oath of confidentiality or decides to ignore other security rules.

A security policy should require that all violations and breaches be reported to the senior officer of the public body.

***Sanctions*:** The security policy should state how an investigation into a violation or breach of security will be implemented. It should also set out any administrative or disciplinary sanctions that will be administered if a breach or violation is found.

Sanctions may consist of the removal of access to sensitive information or information systems, verbal or written reprimand, suspension without pay, or dismissal. The sanction will depend on the circumstances and the record of the officer or employee.

Section 86(1) and (2) of the *FOIP Act* provides that a person must not collect, use or disclose personal information, or attempt to gain, or gain, access to personal information in violation of the *Act*. A person who does so is guilty of an offence and liable of a fine up to $10,000.

***Review and redress*:** A security policy should ensure a fair and equitable process for dealing with individuals who have consented to personnel security checks or are subject to disciplinary action related to security. A clear process for appeal and review should be put in place.

Security in Contracting

Protective arrangements under **Part 2** of the *Act* apply to personal information in the custody or under the control of public bodies. This may include information that is collected, compiled, used, disclosed or disposed of by a contractor.

A security policy should stipulate that its provisions apply to persons working under contract to a public body who are required to handle sensitive personal information or have access to information systems or facilities where such information is handled or stored. The extent of physical, technical and personnel security requirements that a contractor will have to meet will have to be decided on a contract-by-contract basis.

For information on establishing security and other requirements during the contracting process, see *Freedom of Information and Protection of Privacy: Contract Manager's Guide*, published by Information Management and Privacy, Alberta Municipal Affairs.

9.6 DATA SHARING AND DATA MATCHING

Data Sharing

Data sharing means the exchanging, collecting, using or disclosing of personal information by one public body or other organization with another public body or other organization for certain purposes which is carried out using any transmission method and which may take place over any time period.

Data sharing may be used for a variety of purposes, including:

- determining or verifying the eligibility of a client for a program, benefit or service;
- detecting duplicate payment of benefits from two public bodies;
- determining an individual's suitability for an honour or award; and
- delivering a joint program.

There are no specific controls over data sharing in **Part 2** of the *FOIP Act*. However, the collection, use and disclosure provisions of the *Act* govern how such activities can be carried out.

When a public body determines that sharing some of the personal information it holds is necessary, this should be supported by a written data sharing agreement.

Using a data sharing agreement to establish the terms and conditions that will apply to a transfer of personal information has the benefit of:

- providing a formal mechanism for the efficient and timely sharing of personal information;
- limiting the type and amount of personal information that can be disclosed and the purposes for which it can be used; and
- providing additional privacy protection both during and after the sharing by binding the parties to enforceable terms and conditions.

For further information on data sharing, including the components of a data sharing agreement, see *Freedom of Information and Protection of Privacy: Guide to Developing Personal Information Sharing Agreements*, published by Information Management and Privacy, Alberta Municipal Affairs.

Data Matching

Data matching means computerized comparison of one or more data bases or sets of records of personal information held by one public body or organization with one or more other data bases or sets of records held by a different public body or organization, where the computer matching program creates or merges files on identifiable individuals, and where the matched data is used to make decisions about the individuals to whom the data relates.

Data matching tends to involve electronic data because its effectiveness is generally based on the comparison of databases containing large volumes of transactional data.

Related to data matching is *data linkage*, also known as *data profiling*, which is a computerized use of personal data from a variety of sources, including personal information banks, to merge and compare files on identifiable individuals or categories of individuals for administrative purposes. This linkage or profiling activity generates a new body of personal information.

Data matching and data linkage may have a valuable role to play in increasing the efficiency of a wide variety of public body programs. They can, however, also have a major impact on the privacy of individuals.

For this reason, there is a need to balance the requirements for efficiency and effectiveness in public body programs with the potentially invasive nature of the activity, particularly if it involves data linkage. Careful attention needs to be given to the quality and reliability of the data being matched, especially if the purpose of the activity is to pursue administrative actions against individuals.

A *matching program* is a specific procedure that is developed and used to compare a set, or sets, of records containing personal information held by a matching public body with another set, or sets, of records held by a matching source.

It incorporates all stages of the matching process, from the acquisition to the disposal of data. This matching activity may or may not generate a new personal information bank.

A *matching source* is an organization that discloses personal information to a public body for the purposes of a matching program. A matching source may be within the same public body as the matching recipient, another public body or any other organization.

A *matching recipient* is a public body that is planning to conduct, or is conducting, a matching program.

There are no specific controls over data matching in **Part 2** of the *FOIP Act*. However, the collection, use and disclosure provisions do govern how such activities can be carried out.

When carrying out data matching, public bodies should:

- **determine whether the matching is permitted by the collection, use and disclosure provisions of the *Act*;**
- **prior to initiating a matching program, assess the feasibility of the proposed matching, including the potential impact on the privacy of individuals and the costs and benefits of the data matching program;**
- **notify the Information and Privacy Commissioner of a new matching program by providing that Office with a copy of this assessment at least 60 days before the program is to commence;**
- **ensure that data matching programs are authorized by the head of the public body or the designated official to whom this authority has been delegated;**
- **ensure that all matching activities are accounted for in relevant personal information bank descriptions; and**
- **verify information generated by a matching program against original or additional authoritative sources**

before that information is used for an administrative purpose.

These provisions do not need to be applied to matching involving:

- information not used for an administrative purpose directly affecting an individual;
- two or more databases of information collected and held for the same purpose;
- programs that review the contents of a record system to remove or correct items where there is no intention to take administrative action;
- programs that co-locate items previously in separate locations, provided the purposes for which the information collected or compiled continue to apply; or
- information used for research, statistical or program evaluation purposes, if the output is in a form that is not individually identifying.

***Preliminary assessment*:** When considering a data matching program, a preliminary assessment should be carried out to determine whether matching data is the most practical and convenient approach to the need and whether there is a basis for proceeding in **Part 2** of the *FOIP Act*.

Preliminary assessment of a matching program is done by:

- assessing the advantages of the proposed matching program against alternative control, management or enforcement approaches;
- verifying that the collection involved in a matching program is authorized by a statute or regulation of Alberta or Canada, is for the purpose of law enforcement, or relates directly to and is necessary for an operating program or activity of a public body (**section 32**);
- examining the possibility of collecting the information directly from the individual to whom it relates or whether collection through data matching is permissible by virtue of one or more of the following conditions: the individual has authorized indirect collection, the public body could obtain the information from another source without the consent of the individual under **section 33(1)**, or direct collection might result in the collection of inaccurate information (**section 33(3)**);
- determining whether it is necessary to notify individuals of the new use of their personal information, and if so, the best procedures for notification, or if not, the justification for not notifying the individual;
- describing the means for ensuring that the information used in the matching program, as well as the information generated, is accurate and complete (**section 34**);
- determining whether the consent of individuals to the use or disclosure of their personal information is required, and if so, the procedures for obtaining any required consent, or if not, the reason for not obtaining consent;
- setting the start and completion dates for the matching program and, where applicable, the schedule for any required periodic or continuing matching programs;
- describing the results of any pilot projects designed to test the proposed matching programs.

Whenever possible, matching public bodies should test the programs to evaluate their effectiveness; and

- determining the costs and the benefits of the proposed data matching program.

At this stage, the public body should also determine the procedures available to:

- establish a records retention and disposition schedule for information used in matching programs, including the program protocols used to establish the link between sets of personal information;
- ensure that any new use or disclosure of personal information is included in the directory containing descriptions of personal information banks held by the public body; and
- establish a personal information bank for the personal information generated as a result of the matching program.

***Cost–benefit analysis*:** A second step is a basic cost–benefit analysis. Public bodies should determine the costs of a matching program relative to its benefits.

This analysis should be in terms of the level of a public body's resources (e.g., staff, equipment and materials needed to perform a matching program) and the amount of effort required to develop and to implement it.

The importance of the cost–benefit factor to the decision to proceed with a matching program will vary with the context in which the public body operates.

Projected or actual resource expenditures should be examined in relation to direct costs, data processing and telecommunications costs, administrative overhead, and any costs associated with contracting out activities.

The cost–benefit analysis should quantify and document the following savings, as appropriate:

- funds that may be recouped through voluntary repayments or formal collection action;
- savings due to termination of ineligible benefits;
- savings due to the denial of benefits that would otherwise have been approved;
- savings due to the deterrent effect of the program;
- savings relative to other methods of data collection or compilation.

It may be appropriate in some instances to provide evidence of a substantive impact on society or the economy if the program is not implemented.

***Notification of the Information and Privacy Commissioner*:** As a third step, public bodies should consult with the Office of the Information and Privacy Commissioner on matching projects. To allow for this external review before implementation, public bodies should give the Information and Privacy Commissioner advance notification of their intention to initiate a matching program. Providing the Commissioner's Office with the preliminary feasibility assessment may serve this purpose.

A reasonable time frame for such notification is at least 60 days before the matching is scheduled to begin. This ensures that the Office of the Information and Privacy Commissioner is informed of new consistent uses and new data matches.

The Commissioner may make recommendations to the head of the public body if, in his or her opinion, such uses or activities are not in accordance with the provisions of the *FOIP Act*.

Approval: A fourth step is to get final approval for the matching activity or program within the public body that is the matching recipient.

It is recommended that the final approval for a data matching program be given by the head of the public body undertaking the program or by a senior official specifically delegated under the *FOIP Act* to authorize such programs.

When a public body is frequently involved in matching activities and the size and organization of the body merit it, the head may establish an internal review body. This might consist of senior program officials and the FOIP Coordinator. The group would review proposed matching programs for compliance with **Part 2** of the *FOIP Act* and make recommendations to the head concerning matching programs for which the public body is either the matching recipient or the matching source.

Public notification of a matching program: The *FOIP Act* requires that a public body account publicly for the use and disclosure of personal information. One way to do this effectively is to notify the general public, or specific groups of clients, of a matching program.

Public notification is supported by ensuring that there is a current, accurate record of all ongoing data matching activities in the descriptions of personal information banks held by public bodies.

Special conditions relating to the disclosure of information for matching programs: There are a number of factors that a public body that is asked to disclose personal information for data matching purposes (a matching source) must take into consideration.

Disclosure of personal information requested for matching purposes can only be made under the conditions set out in **Part 2** of the *FOIP Act*.

The public body disclosing the information should:

- request and review the preliminary assessment and any other available documentation on the proposed matching to assist in making an informed judgment as to whether the proposed match is justified by program needs as well as the requirements of the *Act*. The public body must be able to demonstrate that it can disclose the information under **section 38** of the *Act;*
- determine whether additional information or action will be required for verification purposes and whether such disclosure or action is acceptable;
- ensure that when a disclosure is made for matching purposes, it is sanctioned by a written agreement

signed by senior officials representing both the matching source and the matching recipient. The agreement should include any further conditions that should apply; and

- ensure that any contract involving a matching program stipulates that the contracted activities will be conducted in accordance with the provisions of the *FOIP Act* and the public body's policy on data matching.

Verification process**:** Good administrative practice dictates that public bodies subject information generated by a matching program to a verification process involving original or additional authoritative sources.

This verification process should be carried out before the information is used in a decision-making process that directly affects an individual. Furthermore, an individual should be given an opportunity to refute the information produced by a matching program before any administrative action concerning the individual is initiated.

Security**:** Personal information and computer systems should be safeguarded from accidental and deliberate threats to confidentiality and to data integrity, including authenticity, accuracy, currency, and completeness. Security safeguards implemented by the matching recipient should be at least equivalent to those of the matching source.

Retention and disposition**:** A matching recipient should establish retention and disposition standards for personal information used and generated by a matching program.

These standards are established through records retention and disposition schedules or agreements.

Chapter 10
Information and Privacy Commissioner

10.1 OVERVIEW

The *FOIP Act* establishes an Information and Privacy Commissioner to monitor compliance by public bodies with the provisions of the FOIP legislation and to investigate complaints. The powers of the Commissioner are set out in **sections 51 to 57** of the *Act*. The role of the Commissioner in conducting reviews and inquiries is set out in **sections 62 to 70**.

10.2 APPOINTMENT

The Information and Privacy Commissioner is an Officer of the Legislature and is independent of government.

Section 43 of the *Act* provides that the Lieutenant Governor in Council, on the recommendation of the Legislative Assembly, appoints the Information and Privacy Commissioner to carry out the duties and functions set out in the *Act*.

The Commissioner is appointed for a term of five years and is eligible for reappointment. The Commissioner may not be a Member of the Legislative Assembly (**section 44**). The Commissioner may resign, but may be removed or suspended from office only for cause or incapacity (**section 45**). This means that the Commissioner may not be removed by arbitrary or capricious action, but only for some reason affecting or concerning the ability or fitness of the Commissioner to perform the duties of the office.

The Lieutenant Governor in Council may designate a judge of the Court of Queen's Bench of Alberta to act as an adjudicator:

- when a FOIP request involves the Information and Privacy Commissioner as the head of the public body, or,
- when, in the Commissioner's opinion, the Commissioner has a conflict of interest in a review or investigation (**section 71**).

The adjudicator has the same powers as the Commissioner in disposing of a review or investigation.

10.3 MANDATE AND POWERS

Part 3 of the *FOIP Act* establishes the position of Information and Privacy Commissioner and a supporting office. This office was established in 1995. The Commissioner has a continuing responsibility to ensure that public bodies are complying with the letter and spirit of the *Act*.

The general powers of the Commissioner are listed in **section 51**.

The Commissioner has general responsibility for monitoring how the legislation is administered to ensure that its purposes are achieved. Specifically, he or she may:

- carry out investigations to ensure compliance with any provision of the *Act* or compliance with rules relating to the destruction of records. This includes destruction in accordance with rules set out in any other enactment of Alberta, in a by-law, resolution or any other instrument by which a local public body acts, or as authorized by the governing body of a local public body (**section 51(1)(a)**);
- make an order regarding duties imposed by the *Act*, administrative matters and the collection, correction, use or disclosure of personal information as described in **section 68(3).** Such an order can be made whether or not a review is requested (**section 51(1)(b)**);
- inform the public about the *Act* (**section 51(1)(c)**);
- receive comments from the public concerning the administration of the *Act* (**section 51(1)(d)**);
- engage in or commission research into anything affecting the achievement of the purposes of the *Act* (**section 51(1)(e)**);
- comment on the implications for freedom of information or protection of personal privacy of proposed legislative schemes or programs of public bodies (**section 51(1)(f)**);
- comment on the implications for protection of personal privacy of using or disclosing personal information for record linkage (**section 51(1)(g)**);
- authorize the collection of personal information sources other than the individual the information is about (**section 51(1)(h)**);
- bring to the attention of the head of a public body any failure to assist applicants under **section 9** (**section 51(1)(i)**); and
- give advice and recommendations of general application to the head of a public body on matters respecting the rights or obligations of a head under the *Act* (**section 51(1)(j)**). The Commissioner may use this power in order to suggest improvement to the way a public body deals with requests. It will likely only be used when there is evidence of poor administration, such as inadequate training or failure to locate records; where there is wanton disregard for the provisions of the *Act*; or where there are systemic problems, such as regular delays, improper interpretation of exceptions or complaints about breaches of privacy.

Further, without limiting the general powers in **section 51(1)**, the Commissioner may investigate complaints from the public that:

- a duty imposed by **section 9** (duty to assist applicants) has not been performed (**section 51(2)(a)**);
- an extension of time for responding to a request is not in accordance with **section 13** (time extensions) (**section 51(2)(b)**);
- a fee required under the *Act* is inappropriate (**section 51(2)(c)**;
- a correction of personal information requested under **section 35(1)** has been refused without justification (**section 51(2)(d)**); and
- personal information has been collected, used or disclosed by a public body in violation of **Part 2** of the *Act* (**section 51(2)(e)**).

The Commissioner has sole jurisdiction to investigate matters of freedom of information and privacy protection that are governed by the *Act*. The *Act* specifically prohibits the Ombudsman from investigating any matter within the jurisdiction of the Commissioner unless the Commissioner agrees (**section 60**).

An order issued by the Information and Privacy Commissioner is *final* (**section 69**). The Courts have their inherent and constitutional jurisdiction to review and determine whether the Commissioner has acted within the authority given to the Office under the *Act*. This is known as the common law principle of *judicial review*.

As an independent Officer of the Legislature, the Commissioner reports annually to the Speaker of the Legislative Assembly describing the work of the Commissioner's Office, any complaints or reviews resulting from a decision of a public body, and other matters relating to freedom of information and protection of personal privacy (**section 61**).

Further information, including copies of brochures, news releases, orders, investigation reports and annual reports, is available at the web site of the Office of the Information and Privacy Commissioner, at www.oipc.ab.ca.

10.4 MONITORING ROLE

A number, but not all, of the powers of the Commissioner are discussed below.

The Commissioner may investigate the administration of the *Act* by public bodies. The Commissioner may also audit the practices of public bodies in the areas of freedom of information and protection of privacy.

In the area of freedom of information, the Commissioner may, for example:

- examine a public body's compliance with the time limits imposed by the *Act*;
- review a public body's compliance with the *Act*'s requirements for third party notification;
- investigate allegations that records are being destroyed to avoid producing them in response to a request under the *Act*;
- investigate whether a public body is acting appropriately in the disclosure of information in the public interest under **section 31**; or
- review the decision of the head of a public body to refuse a request for a fee waiver, if requested to do so by the applicant (**section 87(4.1)**).

In the area of privacy protection, the Commissioner may, for example:

- investigate a public body's disclosures of personal information to third parties to ensure that they are in accordance with the requirements of **section 38** of the *Act*;
- review the collection of personal information by a public body to ensure it has the legal authority to collect the information (**section 32)** or is complying with the rules for indirect collection (**section 33**);
- review the records disposition practices of a public body to ensure that it is retaining personal information as required by **section 34(b)** of the *Act*;

- audit a public body's fair information practices within a program or personal information system to ensure compliance with **Part 2** of the *Act*; or
- investigate the application of new information technology to ensure that privacy rights of individuals are being adequately addressed and protected.

The Commissioner may also examine and comment on legislation and program activities in terms of any implications for freedom of information and protection of privacy.

Examples of such legislation and program activities include:

- the amendment of a statute or by-law to include provisions for introducing personal identifiers, or to allow release of personal information. The Commissioner could examine the public body's reasons for including such amendments and comment on their relationship to the provisions and intent of the *FOIP Act*; and

- the enhancement of service delivery through implementation of a "smart card" using personal information for a variety of purposes. The Commissioner might advise the public body as to the need for a Privacy Impact Assessment for the project.

By commenting on and informing the public about the implications of legislative and other proposals of public bodies, the Commissioner can help them to comply with the spirit of open government and privacy rights and to be accountable for their actions.

The Commissioner may review automated information systems to ensure that they comply with the *Act*.

The Commissioner also has the mandate to conduct or commission research into any issue affecting the way in which the *Act's* purposes are being achieved.

The Commissioner might choose, for example, to hire a consultant to research the implications of testing employees in various local public bodies for drug use or to study the appropriate pricing of information made available without a FOIP request.

The Commissioner's role in dealing with reviews and complaints from persons not satisfied with the handling of a FOIP request or correction of personal information is discussed in section 10.13 of this chapter.

10.5 PROVISION OF ADVICE

The Commissioner may provide the head of a public body with advice and recommendations on matters respecting the rights or obligations of a head under the *Act* **(section 51(1)(j))**. Further, the head of a public body may ask the Commissioner to give advice and recommendations on any matter respecting any rights or duties under the *Act* **(section 52(1))**.

Some examples of advice given under **section 51** have been provided earlier in this chapter.

The Commissioner may include advice or recommendations in an order or an investigation report.

The head of a public body might seek advice from the Commissioner on general procedures or matters of interpretation relating to an access request or on how to appropriately apply the privacy protection provisions of **Part 2** of the *FOIP Act*. The advice will normally be sought through a letter from the head of a public body to the Information and Privacy Commissioner. Advice given in response to a request from the head of a public body must be of a general nature and not anticipate or relate to a specific case. It can include recommendations on the administration and application of the *Act* generally in a particular public body.

Section 52(2) provides that the Commissioner may respond to the head of a public body in writing with advice and recommendations that:

- state the material facts either expressly or by incorporating facts stated by the head;
- are based on these facts; and
- are based on any other considerations that, in the opinion of the Commissioner, are appropriate.

10.6 DISCLOSURE TO THE COMMISSIONER

As discussed in Chapter 6 of this publication, the Commissioner must investigate and review any disclosure made to him or her by a public body employee of any information that an employee is required to keep confidential and that the employee, acting in good faith, believes:

- ought to be disclosed by a head under **section 31** (disclosure in the public interest); or
- is being collected, used or disclosed in violation of **Part 2** of the *Act* (**section 77(1) and (2)**).

The Commissioner must not disclose the identity of the employee to any person without the employee's consent.

In carrying out an investigation and review under this provision, the Commissioner has the powers of investigation, mediation and order-making, as well as the protections provided under **Part 4** of the *Act* (**section 77(7)**).

10.7 POWERS

The Commissioner has all the powers, privileges and immunities of a commissioner under the *Public Inquiries Act* (**section 54(1)**) when conducting an investigation under **section 51(1)(a)** or a review under **Part 4,** or in giving advice and recommendations under **section 52** of the *Act*. These include the power to compel witnesses to attend and answer questions at an inquiry, to compel records to be produced, to hold a person in contempt, and to obtain assistance from law enforcement officers.

10.8 ACCESS TO INFORMATION

The Commissioner may require any record to be produced and may examine any information in a record, including personal information, whether or not the record is subject to the provisions of the *Act* (**section 54(2)**).

A public body must produce any record or copy of a record requested by the Commissioner under **section 54(1)** or **(2)** within 10 days. This must be done regardless of any other enactment of Alberta but not if a federal enactment, such as the *Young Offenders Act* (Canada), prohibits disclosure (see *IPC Order 96-015*). Records must be produced despite any privilege of the law of evidence that might otherwise apply (**section 54(3)**). This requirement applies to records that the public body believes to be excluded from the coverage of the *Act* under **section 4(1)** (see *IPC Practice Note No. 4, Section 4 – Exclusions from the Act*).

If a public body is required to produce a record and it is not practicable to make a copy of it, the head of a public body may request that the Commissioner examine the original at the site of the public body (**section 54(4)**).

The Commissioner must return all records or copies of records to the public body after completing a review or investigating a complaint (**section 54(5)**).

10.9 POWER TO DISREGARD REQUESTS

The head of a public body may, under **section 53** of the *FOIP Act*, request the Commissioner's authorization to disregard requests from an applicant. This applies to both requests for access to information and requests for correction of personal information. The public body must present facts in support of its request. The Commissioner then makes a decision. The head may be allowed to disregard a request if it is:

- repetitious or systematic in nature, and
- processing the request would unreasonably interfere with the operations of the public body, or amount to an abuse of the right to make requests;

or

- frivolous or vexatious.

A request is *repetitious* if it is one in a series of requests by an applicant for substantially the same information or records.

Requests might be viewed as *repetitious* in cases where an applicant:

- continues to apply repeatedly for the same or similar information even though the original request has been disposed of and there is nothing new or different in the responsive records;
- continues to ask for corrections of particular opinions about him or herself when a decision has been made and the record has been annotated;
- makes repeated requests for information which he or she has been advised is available for purchase; or
- makes the same request to a public body before a previous request has been completed or any review or investigation procedure carried out.

A request is *systematic* in nature if it is part of an extensive pattern of related requests by an applicant or a group of applicants.

Requests might be considered *systematic* in nature when a single applicant or a group of applicants:

- makes a large number of the same or similar requests; or
- regularly makes a request and then, after receiving a fee estimate, splits up the request into several separate requests to avoid fees.

A public body may only request authorization to disregard repetitious or systematic requests if processing the request would *unreasonably interfere with the operations of the public body* or *amount to abuse of the right of access*.

Unreasonable interference with the operations of a public body might be demonstrated by showing the impact that particular repetitious or systematic requests are having on the resources needed to respond within a public body and the actual costs of providing a response.

Abuse of the right of access arises when the action of an applicant is demonstrably a misuse of the *FOIP Act*. It may be obvious that requests are not being made to obtain information or achieve a legitimate correction of information, but rather to tie up the resources of the public body or frustrate the administration of a particular program or activity.

A request may be *frivolous or vexatious* if it has no sound basis in fact or is malicious. The applicant may not be making repeat requests or abusing his or her rights of access under the *Act*, although that may be the case.

Public bodies might support an argument that a request is frivolous or vexatious with reference to a past pattern of conduct that indicates an abuse of the process for access or with evidence that shows that the request is made in bad faith or for a purpose other than to obtain access to information.

Examples of requests that might be considered frivolous or vexatious include:

- continual requests for records that a public body has already established it does not have;
- requests involving fees made by an applicant who has demonstrated a pattern of abandoning a request whenever a fee waiver is not granted or the Commissioner upholds a fee;
- requests that show an intention to harass a public body, to "break" the system or to engage in "information warfare."

In one case from another jurisdiction, for example, it was reported that an applicant made a large number of requests to public bodies and had 75 reviews and privacy complaints before the Commissioner's office.

When requesting the Commissioner's decision in such a case, the public body might provide evidence of the considerable costs and time involved in dealing with a particular applicant or group of applicants.

No single factor will determine whether a request is frivolous or vexatious. Public bodies need to present a case based on the history of requests by an applicant and the context of those requests when asking for permission to disregard a request.

Asking for authorization to disregard requests should be rare. Public bodies should ensure that they have fully discharged their duty to assist applicants in a full and forthright manner and have a strong case before seeking permission from the Commissioner to disregard requests from one or more applicants.

10.10 STATEMENTS PROVIDED TO THE COMMISSIONER

A statement made or an answer given by a person during an investigation or inquiry by the Commissioner is inadmissible in evidence in court or in any other proceeding, except:

- in a prosecution for perjury in respect of sworn testimony;
- in a prosecution for an offence under the *FOIP Act*; or
- in an application for judicial review or an appeal from a decision of that review (**section 55(1)**).

These conditions also apply to evidence from proceedings conducted before the Commissioner (**section 55(2)**).

Anything said, any information supplied or any record produced by a person during an investigation or inquiry by the Commissioner is privileged. The rules that apply are those for a proceeding before a court (**section 56**).

Section 57 of the *Act* places restrictions on the disclosure of information by the Commissioner and the staff of the Office of the Commissioner. They must not disclose any information they obtain in the performance of their duties, with the following exceptions:

- the Commissioner may authorize disclosure of information that is necessary for the conduct of an investigation under the *Act* or to establish the grounds for findings and recommendations made under the *Act* (**section 57(2)**);
- the Commissioner may disclose to the Minister of Justice and Attorney General information relating to the commission of an offence against an enactment of Alberta or Canada, if the Commissioner believes there is enough evidence to justify such disclosure (**section 57(4)**); and
- the Commissioner may authorize disclosure of information in the course of a prosecution for perjury or for an offence under the *Act*, or in an application for judicial review or an appeal arising from that application (**section 57(5)**).

This section allows the Commissioner to request that the police lay charges under **section 86** of the *Act*.

During the conduct of an investigation, inquiry or audit, the Commissioner and the staff of the Commissioner's Office must not disclose any information that the head of a public body would be required or authorized to withhold from disclosure. They must also ensure that they do not disclose the fact that information exists where, in the notice of refusal to provide access, the public body did not indicate whether or not the information existed (**section 57(3)**).

10.11 PROTECTION FROM LIABILITY

The Commissioner and the staff of the Commissioner's Office are not liable for anything they do in good faith in the exercise of their duties under **Part 3**, Office and Powers of the Information and Privacy Commissioner, and **Part 4**, Review and Complaints, of the *Act* (**section 58**).

As long as the Commissioner and his or her staff act honestly and with the intention of complying with the *Act*, no action can be brought against them.

10.12 DELEGATION OF THE COMMISSIONER'S POWERS

Section 59(1) provides that the Information and Privacy Commissioner may delegate, in writing, to another person any duty, power or function of the Commissioner under the *Act*. The only exception to this provision is that the Commissioner cannot delegate the power to delegate.

This allows the Commissioner to delegate the power to examine law enforcement information and Cabinet documents, to authorize public bodies to disregard requests and to hold inquiries and issue orders on completion of those inquiries.

10.13 REVIEWS AND INVESTIGATIONS

Reviews

Section 62 of the *FOIP Act* provides persons who have made a FOIP request with the right to ask the Information and Privacy Commissioner to review any decision, act or failure to act by a public body (**section 62(1)**).

Third parties have the right to ask the Commissioner to review the decision of a public body to provide access to records that might harm their personal privacy or business interests. The public body's decision in response to a request for third party information may be either to grant access to all or part of a record containing this information, or not to grant access. If the public body decides to grant access, the third party may request a review before any records or parts of records are disclosed (**section 62(2)**).

A person who believes that his or her personal information has been collected, used or disclosed in violation of **Part 2** of the *Act* may also ask the Commissioner to review the matter (**section 62(3)**).

A relative of a deceased individual may ask the Commissioner to review a decision of a public body under **section 38(1)(aa)** not to disclose personal information about the deceased individual (**section 62(3.1)**).

The right to an impartial review of decisions or actions of a public body is fundamental to guaranteeing freedom of information and protection of privacy rights. The review mechanism ensures that these rights are interpreted consistently among public bodies and the purposes of the *Act* are achieved. The orders, which summarize the reviews, issues, reasons, and findings of the Commissioner, also provide guidance to public bodies regarding the proper interpretation of the *Act*.

A review by the Commissioner of the decision of a public body is intended to be an avenue of last resort. In most cases, a person will be satisfied that the public body has acted responsibly and any outstanding issues can be settled between the public body and the person concerned. Even in cases where the person asks the Commissioner to review a decision, issues can often be settled through mediation and an inquiry may not be necessary.

Certain matters that may be the subject of a request for review can also be grounds for a complaint to the Commissioner under **section 51(2)** of the *Act*.

These are:

- matters relating to the public body's duty to assist the applicant (**section 9**);
- a decision to extend the time limit under **section 13** for responding to a request;
- the amount of a fee charged or the refusal to waive all or part of a fee under **section 87;**
- a refusal to make a correction to personal information as requested under **section 35(1)**; and
- the collection, use or disclosure of personal information in violation of **Part 2** of the *Act*.

Requesting a Review

Section 63 of the *Act* sets out the process for requesting a review. A **Flowchart of the Review Process** is provided in ***Figure 13***. The Office of the Information and Privacy Commissioner provides a **Request for Review Form** for this purpose. A copy of the form is included in Appendix 6 of this publication.

Applications for a review can be made on this form or by letter, but in all cases must be *in writing*. **Section 79** establishes classes of individuals who may act for deceased persons, incompetent persons, minors and any other individuals in exercising this right under the *Act*.

A person must deliver a request for a review to the Commissioner within 60 days of receiving notification of a public body's decision or a longer time when allowed by the Commissioner (**section 63(2)(a)**). Third parties have only 20 days in which to seek a review (**section 63(2)(b)**).

Failure by a public body to respond in time to a request for access to a record is treated as a decision to refuse access (deemed refusal). In this case, there is no notification by the public body.

Preparation for a Review

A public body must be able to show that it has properly fulfilled its duties under the *Act*. It should document the reasons for each decision relating to the withholding of records or parts of records and should ensure that the circumstances surrounding the request support each action it takes.

To reduce the need for review of decisions, public bodies should provide applicants and third parties with clear explanations of their decisions, the provision(s) of the *Act* that apply and the reasons why they are applicable in the particular instance. These explanations provide a basis for discussion of the decision and may help the public body and the person to settle any outstanding issues without recourse to the Office of the Information and Privacy Commissioner. This point is discussed in *IPC Practice Note No. 2, Informing the Applicant of Grounds for Refusal*. If a particular case for review deals with an issue that has implications across government or affects most public bodies, the public body should consult with Information Management and Privacy, Alberta Municipal Affairs.

Review Process

The Office of the Information and Privacy Commissioner has developed procedures for conducting reviews and public inquiries and these are available from that office.

IPC Practice Note No. 5, Preparing Records and Submissions for Inquiries should also be carefully read. The *Act* has enabling provisions and some requirements governing the review process.

Upon receiving a request for review, the Commissioner must provide a copy of the request to the head of a public body and to any other person the Commissioner deems appropriate (**section 64(1)**).

The Commissioner may sever any information in the request that is considered appropriate before providing copies as stated above (**section 64(2)**). This is necessary because applicants may include personal information as a part of their requests for review, and it may not be appropriate to disclose this to the public body or other persons.

The staff of the Commissioner's Office, the public body and the applicant will jointly review the request to determine whether or not the concerns raised in it can be addressed through mediation.

The Commissioner will also likely ask the public body to submit copies of the following documentation, where applicable:

- the FOIP request;
- notice of the public body's decision;
- any correspondence related to the request, issue or decision;
- an index of the relevant records and exceptions relied upon;
- severed and unsevered copies of the records; and, where applicable,
- descriptions of personal information in the public body's personal information banks and policies and procedures for its management under **Part 2** of the *Act*.

The public body will initially be more familiar with the issues involved than the Office of the Commissioner. If the public body has any information concerning affected persons who should be notified of the review, it should inform the Commissioner's Office as soon as possible.

It should also make known any relevant issues, considerations or factors that affected the making of the particular decision. The Commissioner will have a better understanding of the public body's position if it can demonstrate that it made every effort to meet a person's needs and to resolve outstanding issues.

Mediation

Section 65 provides that the Commissioner may authorize a mediator to investigate and try to settle any matter that is the subject of a request for a review. In most cases, the Commissioner will instruct a Portfolio Officer to proceed in this way. The mediator does not impose a settlement. Rather, mediation is intended to help the public body and the person requesting a review to arrive at a settlement before a formal inquiry is initiated.

Inquiry

If a mediator is not appointed or the matter is not resolved with the help of a mediator, the Commissioner normally conducts an inquiry (**section 66**).

In the course of the inquiry, the Commissioner will decide all questions of law and fact.

The Commissioner's powers in conducting inquiries are provided in **sections 54** and **66** of the *Act*.

The Commissioner has broad discretion to determine how an inquiry will be conducted. It may be conducted in private (**section 66(2)**) and the Commissioner may decide whether representations are to be made orally or in writing (**section 66(4)**).

The person who asked for the review, representatives of the public body concerned and any person given a copy of the request for review are entitled to make representations to the Commissioner during the inquiry (**section 66(5)**). They may choose to be represented by counsel or an agent.

No party has a right to be present during another party's representations, to have access to or to comment on representations made by another person during the inquiry process (**section 66(3)**).

In the case of a refusal of access, the Commissioner has the right and duty to view all records that have been withheld from disclosure in whole or in part. This right pertains regardless of the exception that the public body has used or the fact that the public body believes the records are excluded from the scope of the *Act*.

The Commissioner may require the records to be produced within 10 days (**section 54(3)**). The Commissioner must return such records to the public body upon completion of the review (**section 54(5)**).

The head of a public body may require the Commissioner to examine a record at the site at which it is being held, if it is not practical to make a copy (**section 54(4)**). This could occur, for example, when a record is too fragile to copy or the copying process would damage the record. Public bodies should avoid, as much as possible, requiring on-site examination of records since it will place an additional administrative burden on their own and the Commissioner's operations.

The Commissioner may compel witnesses to attend an inquiry and answer questions. The Commissioner has all the powers of a Commissioner provided under the *Public Inquiries Act*. These include the power to hold a person in contempt and to obtain the assistance of law enforcement officers to compel attendance at an inquiry or to compel records to be produced.

Refusal to Conduct Inquiry

Over time, issues raised in requests for review may replicate issues already dealt with by the Commissioner. If the Commissioner believes that the subject matter of a request has already been dealt with in an order or an investigation report, the Commissioner may refuse to conduct an inquiry (**section 66.1**).

Time Limits for Review

Normally, the Commissioner's inquiry must be completed within 90 days after receipt of the request for review (**section 66(6)**). This time limit encompasses all elements of the review process, including mediation and any formal inquiry.

However, the Commissioner may notify all parties to a review that he or she is extending the period for the review and establish a date for the completion of the review (**section 66(6)**). The intent of the *Act* is to ensure that an independent review of decisions can take place, so even if the process is not completed within the extended time limit, the Commissioner has the power to complete the inquiry (see *IPC Order 99-011*).

Burden of Proof

Section 67 establishes where the burden of proof lies in various situations relating to access to records. Normally, the burden of proof rests with the public body refusing access to all or part of a record (**section 67(1)**), unless the request is for a record or part of a record that contains personal information about a third party.

This means that under normal circumstances the public body must prove, on the balance of probabilities, that particular information may be excepted from release under the *Act* or excluded from its scope.

Careful documentation of the reasons for refusing the request will form the central arguments that will meet the burden of proof.

A public body also has the burden of proof in cases where an applicant has requested a review of fees charged (see *IPC Order 99-014*). This is because the public body has all the information about the assessment and calculation of fees.

When a public body has refused to disclose personal information under **section 16**, which requires public bodies not to disclose personal information if the disclosure would be an unreasonable invasion of an individual's privacy, the burden of proof rests with the party requesting disclosure of the personal information.

The applicant requesting the personal information must show that disclosure would not be an unreasonable invasion of the personal privacy of the individual to whom the information relates (section 67(2)).

When a third party has requested a review of a public body's decision to disclose a record or part of a record containing personal information about the third party, the burden of proof also lies with the applicant who has requested disclosure of the personal information.

The applicant must show that disclosure will not constitute an unreasonable invasion of the privacy of the individual the information is about (**section 67(3)(a)**).

The applicant also has the burden of proof in the case of a review of a refusal to correct personal information under **section 35.1** (see *IPC Order 98-010*).

When the inquiry concerns a public body's decision to disclose third party business information (**section 15**), the burden of proof lies with the third party resisting disclosure. That is, the third party must demonstrate that the applicant has no right of access to the record (**section 67(3)(b)**).

Commissioner's Orders

Upon completion of an inquiry, **section 68** of the *Act* requires the Commissioner to make an order. If the inquiry concerns a refusal to grant access to all or part of a record, the Commissioner must order one of the following:

- require the public body to give access to all or part of the record;
- confirm the decision of the public body or require the head to reconsider a decision to refuse disclosure; or
- require the head to refuse access to part or all of the record requested.

When the Commissioner finds that a refusal to grant access is in compliance with the *Act*, and the head has properly exercised his or her discretion, the Commissioner may only confirm the decision of the public body or request that the head reconsider the decision based on his or her exercise of discretion.

The Commissioner can only require the head of a public body to reconsider a decision to *refuse* access, not a decision to *grant* access (see *IPC Order 98-001*).

If the inquiry concerns any other matter, such as the matters discussed in **section 51(2)**, the Commissioner may make an order requiring compliance with the provisions of the *Act*.

Section 68(4) provides that the Commissioner may attach any terms or conditions to an order. A copy of the order is given to the person who asked for the review, the head of the public body concerned, any person given notice of the review under **section 64** of the *Act*, and the Minister responsible for the administration of the *Act*.

The head of a public body that has received an order from the Commissioner must comply with the order no earlier than 45 days after the order, and no later than 50 days after the order (**section 70(1)**). This is to allow an applicant, a third party or the public body time to apply for judicial review. If an application for judicial review is made, the Commissioner's order is stayed until the Court has dealt with the application (**section 70(4)**).

There is no appeal from an order made by the Commissioner (**section 69**), except a limited appeal through judicial review (see section 10.14 of this chapter).

It is an offence to fail to comply with an order made by the Commissioner under **section 68**. The Commissioner may choose to file a copy of an order with the clerk of the Court of Queen's Bench and, after filing, the order is enforceable as a judgment or order of that Court (**section 68(6)**).

Investigations

Section 51(1) of the *FOIP Act* enables the Commissioner to monitor compliance with the *Act* and carry out investigations into how the *Act* is being administered to ensure that its purposes are achieved. **Section 51(2)**, without limiting these more general powers, enables the Commissioner to investigate and attempt to resolve complaints that:

- a duty imposed by **section 9** (duty to assist) has not been performed;
- an extension of time for responding to a request is not in accordance with **section 13**;
- a fee under the *Act* is not appropriate;
- a correction of personal information requested under **section 35(1)** has been refused without justification; and
- personal information has been collected, used or disclosed by a public body in violation of **Part 2** of the *Act*.

The main difference between an investigation and a review is that an investigation may not be a result of a FOIP request. A complaint that does not arise from a FOIP request is most likely to occur in cases involving disclosure in the public interest or allegations of improper collection, use or disclosure of personal information.

When an investigation is held into an alleged breach of privacy (**section 51(2)(e)**), a Portfolio Officer in the Commissioner's Office is assigned to investigate the matter. When the investigation is complete, an investigation report is prepared and sent to both parties. It includes the Portfolio Officer's findings and recommendations. The complainant is asked whether the report satisfies his or her concerns and the public body is asked to inform the Portfolio Officer how it will comply with the recommendations.

If the complainant is satisfied with the report's finding and recommendations, and the public body accepts the recommendations, the Portfolio Officer forwards the report to the Commissioner and advises that the complaint has been resolved.

If the complainant is not satisfied with the findings and recommendations, he or she can request that the matter proceed to inquiry in accordance with **section 62(3)**. In this case, the report of the Portfolio Officer is not forwarded to the Commissioner and is not publicly released. Evidence collected during the investigation is not normally forwarded to the Commissioner for the inquiry.

For further details on the process of dealing with complaints see *IPC Practice Note No. 7, Privacy Complaints – Investigations and Inquiries*.

Public bodies are always informed by the Office of the Information and Privacy Commissioner as to whether an issue is subject to a review (**section 62**) or an investigation (**section 51**). The preparation and response to an investigation will be very similar to those outlined for the review process described above (see *IPC Practice Note No. 3, Complaints about Public Bodies – "Reviews" versus "Investigations": Sections 51(2) and 62(1)*).

Time Limits on Complaints

When an investigation arises from a FOIP request, the applicant must deliver the complaint to the Commissioner within 60 days of receiving notification of the public body's decision (**section 63(2)(a)**). A longer time may be allowed by the Commissioner (**section 63(2)(b)**). When allowing a delay, the Commissioner will consider all relevant circumstances.

The *Act* does not specify a time limit for privacy complaints, since these do not, for the most part, arise from a FOIP request. They tend to stem from a complainant's belief that there has been improper collection, use or disclosure of personal information.

Privacy Investigations and Audits

The Commissioner can take an active role in investigating compliance with **Part 2** (Protection of Privacy) of the *Act*. An investigation can be undertaken as a result of a complaint that personal information is not being collected, used, disclosed or protected in accordance with the provisions of the FOIP legislation.

As well, the Commissioner may decide to conduct an audit of privacy protection in a program of a public body that has custody or control of sensitive personal information. The Commissioner's practice is to make all Investigation Reports and Privacy Audit Reports public.

Appendix 4 of this publication contains a checklist of criteria to help public bodies determine whether they currently comply with the requirements of **Part 2** of the *Act*. It also serves as a guide for remedial measures that may be necessary to adequately protect the personal information in the custody or under their control of public bodies.

10.14 ADJUDICATOR PROCESS

Section 71 provides for the appointment of an adjudicator. This occurs in situations when the Information and Privacy Commissioner is not in a position to conduct a review because there would be an apprehension of bias. This can occur when the Commissioner has worked for or been a member of a public body in a capacity directly related to the matter under review, or when the matter relates to the Commissioner's Office or any other Office of which he or she is the head.

The determination that the Information and Privacy Commissioner has a conflict of interest is made by the Commissioner.

An adjudicator cannot review an order of the Information and Privacy Commissioner (**section 71(1.1)**).

An applicant or third party seeking a review under these circumstances may request under **section 74(1)** of the *Act* that an adjudicator be appointed to conduct the review.

The request under must be in writing to the Minister responsible for the *FOIP Act*. The request must be made within 60 days of the person receiving notice of the decision to be reviewed, or 20 days if a third party is challenging disclosure of information. The adjudicator may decide that a longer period should be allowed.

Upon receipt of the request, Information Management and Privacy, Alberta Municipal Affairs, will confirm with the Commissioner's Office that a conflict exists and will verify that the request is valid. Documentation needed to allow the Minister and Cabinet to review the request will be compiled. Alberta Justice is responsible for requesting the Chief Justice of Alberta to nominate a judge of the Court of Queen's Bench to act as adjudicator.

A submission is made to Cabinet to authorize the Lieutenant Governor in Council to designate the judge to act as an adjudicator. The Minister must provide a copy of the applicant's request for review, together with a summary of the review procedures that will govern the process, to the adjudicator, the Information and Privacy Commissioner and any other person affected by the request.

An adjudicator has the same powers and duties as the Commissioner and can dispose of a matter in the same way. A copy of the adjudicator's order must be given to the Commissioner. An order made by an adjudicator is final (**section 76**).

The Minister responsible for the *FOIP Act* is responsible for paying the adjudicator's expenses related to the adjudicator's inquiry.

10.15 JUDICIAL REVIEW

The Information and Privacy Commissioner has exclusive jurisdiction to conduct a review and investigate complaints against a public body under the *FOIP Act*. Courts do not have the power to issue orders under the *Act*.

However, a person may apply to the Court of Queen's Bench of Alberta to exercise its inherent jurisdiction to review any action or failure to act on the part of the Information or Privacy Commissioner. It may also review the decisions of the Commissioner for an error of law on the face of the record, jurisdictional error or breach of natural justice (fairness).

Application for judicial review of a decision of the Commissioner must be made not later than 45 days after the party applying for judicial review is given a copy of the decision.

The Court has the power to compel the Commissioner to do something or to refrain from doing something and the power to send a matter back to the Commissioner for reconsideration.

A judicial review is not an appeal of the Commissioner's decision. The Court cannot substitute its own decision for that of the Commissioner. The Commissioner is the final arbiter of questions of fact but is always subject to the overriding jurisdiction of the Court to ensure that the Commissioner acts within his or her authority.

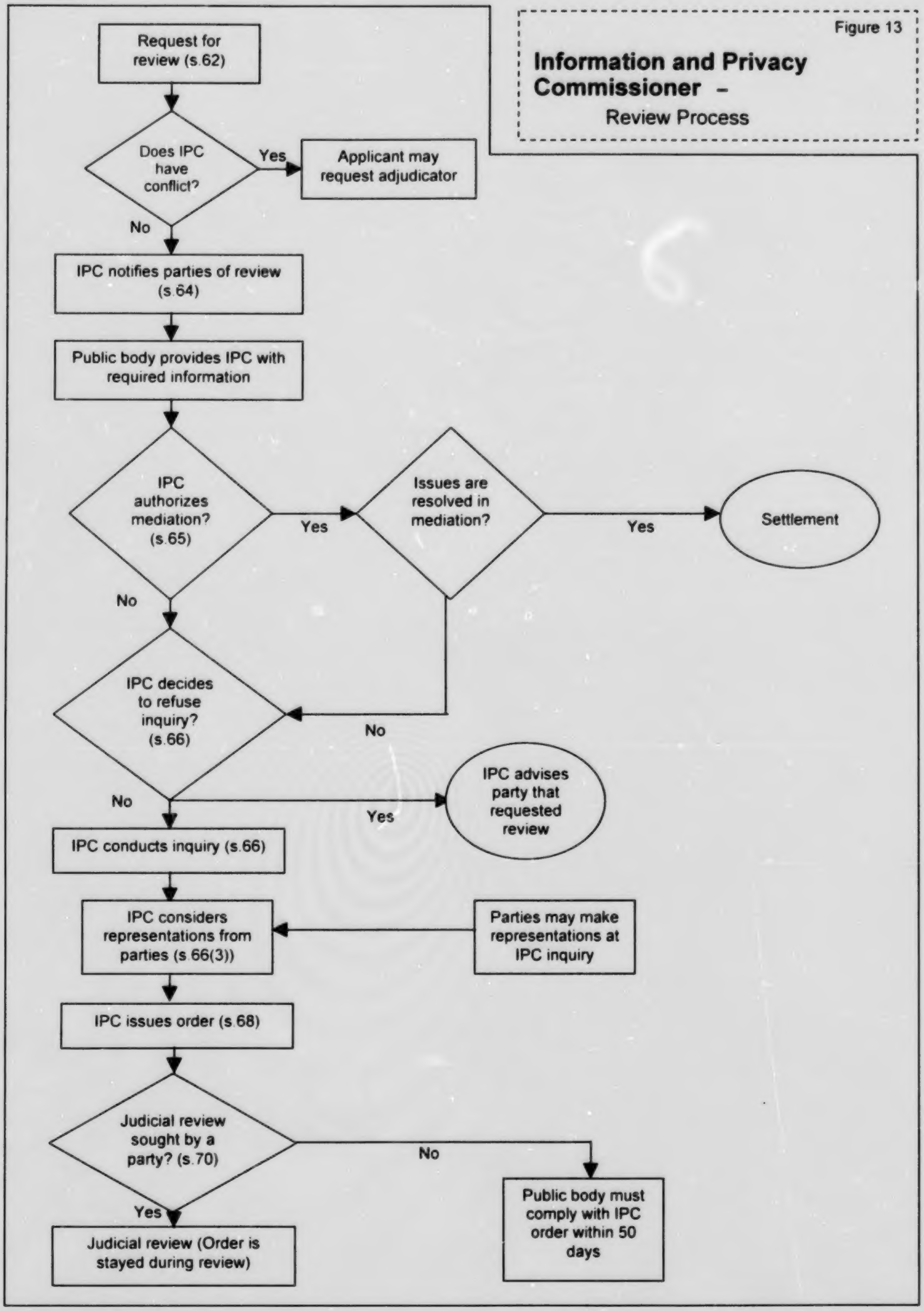


Figure 13

Information and Privacy Commissioner –

Review Process

Request for review (s.62)
Does IPC have conflict?
Yes
Applicant may request adjudicator
No
IPC notifies parties of review (s.64)
Public body provides IPC with required information
IPC authorizes mediation? (s.65)
Yes
Issues are resolved in mediation?
Yes
Settlement
No
No
IPC decides to refuse inquiry? (s.66)
No
Yes
IPC advises party that requested review
IPC conducts inquiry (s.66)
IPC considers representations from parties (s.66(3))
Parties may make representations at IPC inquiry
IPC issues order (s.68)
Judicial review sought by a party? (s.70)
No
Public body must comply with IPC order within 50 days
Yes
Judicial review (Order is stayed during review)

Appendix 1

Definitions

Appendix 1
Definitions

This appendix contains a glossary of terms commonly used in administering the *Freedom of Information and Protection of Privacy Act*. The list of terms included here is selective and those formally defined in the legislation are marked with an asterisk (*). In some cases, the definition of a term is specific to the particular section of the Act where it applies or to the discussion within this publication of the meaning of the term within the context of a particular provision.

***access*:** means the availability of records of a public body for a person to view, study and/or copy the records of a public body. The *Act* provides any person with a right of access to the records in the custody or under the control of a public body.

***adjudicator*:** is a judge of the Court of Queen's Bench of Alberta designated by the Lieutenant Governor in Council to investigate complaints against the Information and Privacy Commissioner as the head of a public body and to review any decision, act or failure to act of the Commissioner as the head of a public body. An adjudicator may also be appointed when the Information and Privacy Commissioner cannot act because of a conflict of interest.

***applicant**:** means any person who makes a request under the *Act* for access to a record or to personal information.

***burden of proof*:** means the obligation to bring forth sufficient evidence or proof to convince the Information and Privacy Commissioner of the truth of a fact.

***Cabinet*:** is the common name for the Executive Council. It consists of a committee of Ministers and Associate Ministers which acts collectively with the Premier to decide matters of government policy.

***Commissioner**:** means the Information and Privacy Commissioner appointed under **Part 3** of the *Act*. The Commissioner is an Officer of the Legislature and is independent of government. The powers of the office are detailed in Chapter 10 of this publication.

complaint: means an expression of dissatisfaction with treatment under the *Act* submitted by an applicant or other person to the Information and Privacy Commissioner. A complaint may be based on one or more of the grounds specified in **section 51(2)** of the *Act:*

- a public body has not met its duty to assist;
- a public body's extension of time for responding to a request is not in accordance with the *Act*;
- a fee charged by a public body is inappropriate;
- a correction of personal information has been refused without justification; or
- personal information has been collected, used or disclosed by a public body in violation of **Part 2** of the *Act*.

consultation: means the process by which a public body asks employees within the body, other public bodies, individuals, and/or third parties (including other levels of government) to comment on a request for access to information in which they have an interest. It also refers to the process of notifying third parties under **Part 1, Division 3** of the *Act*.

continuing request: means an access request that continues to be in effect for up to two years. A delivery schedule is established with the applicant's agreement, and the request is reactivated at intervals set out in the schedule. Each time the request is processed, records newly in the custody or under the control of the public body since the last delivery are provided to the applicant.

control: means the power or authority to manage, restrict, regulate or administer the use or disclosure of a record. A record that is in the possession of or held by a public body, whether at its headquarters, regional or other office, either within or outside Alberta, in the Alberta Records Centre or other records storage centre, or in the offices of a contracted agent is presumed to be under its control unless there is evidence to the contrary.

custody: for the purposes of the *Act*, means having physical possession of a record.

delegation: means the process by which the head of a public body authorizes an employee or officer within the public body to exercise part of the head's authority under the *Act*.

directory of records: is the information required under **section 82** of the *Act* to assist the public in identifying and locating records and personal information.

***disclosure*:** means the act of providing access to records or personal information. In the case of personal information, it generally means providing access to someone or some agency other than the individual to whom the information relates. **Sections 38** to **41** of the *Act* control the disclosure of personal information to third parties. **Section 77** provides a process where an employee may disclose to the Information and Privacy Commissioner information which the employee is required to keep confidential and that the employee, acting in good faith, believes ought to be disclosed in the public interest. This section also allows an employee to disclose to the Commissioner personal information that he or she believes is being collected, used or disclosed in violation of **Part 2** of the *Act*.

***discretion*:** means the exercise of judgment by someone with authority to make a decision under various provisions of the *Act*, where discretion is permitted. The head or delegated official must be able to demonstrate that all relevant factors have been considered in making a particular decision. The public body must be able to demonstrate that it exercised the discretion in a fair and responsible manner. For example, if the public body as a rule or policy excepts all records to which a discretionary exception may apply, the Information and Privacy Commissioner may require the public body to review its application of the discretionary exception.

employee*: means, in relation to a public body, somebody employed by that public body, and includes a person who performs services for the public body as an appointee, volunteer, student or under a contract or agency relationship with the public body.

***enactment*:** means an Act or a regulation or any portion of an Act or regulation. An enactment of Alberta includes a Treasury Board directive (FOIP Regulation, **section 1(3)**).

***exceptions to disclosure*:** are provisions of the *Act* which either require or permit refusal of the right of access to records or personal information in the custody or under the control of a public body. The *Act* establishes limited and specific exceptions to the right of access where disclosure would reveal certain categories of information or would result in harm to the Government of Alberta, the public body or a third party. These exceptions, which are either mandatory or discretionary, are set out **sections 15** to **28** of the *Act*.

***extension*:** means the lengthening of the 30-day time limit imposed by the *Act* for responding to an access request. An extension can only be claimed if:

- the applicant does not provide enough details to enable the record to be located;
- a large number of records are requested or must be searched;
- more time is needed to consult a third party or other public body;
- a third party requests a review under **sections 29** and **30** of the *Act*; or
- there are multiple concurrent requests made by the same applicant, or by 2 or more applicants who work for the same organization or who work in association with each other. The Commissioner has to approve extensions in these cases.

***fees*:** are the charges that an applicant pays to a public body for services related to the processing of an access request. The FOIP Regulation sets out the services for which fees may be charged and the maximum charges for providing these services. Fees may not exceed the actual cost of providing the service.

***Freedom of Information and Privacy Coordinator*:** is the position within a public body responsible for the overall management of its freedom of information and protection of privacy functions and responsibilities.

***FOIP*:** is the official abbreviation for Freedom of Information and Protection of Privacy.

***governing body**:** in relation to a post-secondary educational body means:

- the board of governors or the general faculties council of a university; and
- the board of governors or the academic council of a college or technical institute.

The definition only applies to **sections 4, 22(1)(b) and 88(1)(k)** of the *Act*.

***harm*:** means damage or detriment. It is a term used in relation to the *Act* to describe the injury to a particular public or private interest that could occur as the result of the disclosure of certain types of information in records in the custody or under the control of a public body. A public body may decide to apply an exception for particular information if there is a likelihood that harm will result from disclosure. The public body must be able to provide convincing evidence that disclosure of the requested information would harm the particular public or private interest involved.

***head**:** in relation to a public body, means:

- for a department, branch or office of the Government of Alberta, the member of the Executive Council who presides over it;
- if the public body is one designated in the regulations, the person designated by the Minister responsible for that body to act as the head of that body or, if a head is not so designated, the person who acts as the chief officer and is charged with the administration and operation of that body;
- for a local public body, the person or group of persons designated under **section 89(a)** as the head; and
- for any other case, the chief officer of the public body.

***in confidence*:** is a term applied to information which is furnished with the intent that it be kept secret. In the context of the *Act*, the concept is applied to information or records supplied to a public body by third parties (individuals and other levels of government) or by confidential sources relating to law enforcement. It is a factor in considering exceptions to information under **sections 15, 16, 17(3), 18, 19(1)(d), and 20(1)(b).**

The information must have been supplied in the expectation that the public body would not disclose it. The intention that the confidence will be maintained may be explicitly stated within the record in question or may be implied by the circumstances under which the information was submitted and received. Where confidentiality is implied, there must be objective grounds to support the assumption of confidentiality.

***inquiry*:** is a process used by the Information and Privacy Commissioner to conduct a review requested under the *Act*. Inquiries may be conducted through written submissions or through oral presentations, which may be open to the public. In conducting an inquiry, the Commissioner has all the powers provided under the *Public Inquiries Act*.

***judicial administration record**:** means a record containing information relating to a judge of the Court of Appeal of Alberta, the Court of Queen's Bench of Alberta, or the Provincial Court of Alberta, or to a master of the Court of Queen's Bench of Alberta or a sitting justice of the peace or a presiding Justice of the Peace under the *Justice of the Peace Act*, and includes:

- the scheduling of judges and trials;
- the content of judicial training programs;
- statistics of judicial activity prepared by or for a judge; and
- any record of the Judicial Council established under Part 6.1 of the *Judicature Act*.

***judicial review*:** is the power of the Court of Queen's Bench to determine whether the Information and Privacy Commissioner has acted strictly within the powers that have been given to him or her. Such a review is not an appeal. It does not allow the court to substitute its decision for that of the Commissioner except in exceptional circumstances where the Commissioner's decision is found to be patently unreasonable. A party to an inquiry by the Commissioner may apply for judicial review on jurisdictional grounds or on the basis of an error in law.

***law enforcement**:** for purpose of the *Act*, means:

- policing, including criminal intelligence operations;
- a police, security or administrative investigation, including the complaint that give rise to the investigation, that leads or could lead to a penalty or sanction being imposed. The penalty or sanction could either be imposed by the public body conducting the investigation or by another body to which the results of the investigation are referred; or
- proceedings that lead or could lead to a penalty or sanction being imposed by the body conducting the proceedings or by another body to which the results of the proceedings are referred.

***legal proceedings*:** are proceedings governed by rules of court or rules of judicial or quasi-judicial tribunals that can result in a judgment of a court or a ruling by a tribunal. Legal proceedings include all proceedings authorized or sanctioned by law, and brought or instituted in a court or legal tribunal, for the acquiring of a right or the enforcement of a remedy.

***local public body**:** means an educational body, a health care body or a local government body.

***meeting*:** means a meeting in its entirety or a portion of a meeting (FOIP Regulation, **section 1(4)**).

***Minister responsible for the Act**:** means the member of the Executive Council charged by the Lieutenant Governor in Council with the administration of the *Act*. The Minister currently responsible for the *Act* is the Minister of Municipal Affairs.

***non-arm's length transaction**:** is, for purposes of **section 4(1)(m)** and **(n)** of the *Act*, any transaction that has been approved by:

- the Executive Council or any of its committees;
- the Treasury Board or any of its committees; or
- a member of the Executive Council.

This definition does not apply to **section 15**.

***notice*:** is an official document required to be delivered to a member of the public, an affected third party, or an applicant in particular circumstances under the *Act*. Notice is required:

- for an affected third party where there is an intention to provide access to information which might be excepted under **sections 15** or **16** (**sections 29(1)(2)** and **(3)**);
- to an applicant, when the requested information might be excepted under **sections 15** or **16** and the third party has been notified (**section 29(4)**);
- to both the applicant and third party of the decision on disclosure or exception of the third party's information (**section 30(2)**);
- to the person concerned when his/her personal information is disclosed under **section 16(2)(b)**;
- to an applicant when his or her request is transferred to another public body under **sections 14(1) or 35.1(1)**;
- to a third party whose information is disclosed in the public interest under **section 31** of the *Act* (**section 31(2)** and **(4)**).

offence*: means an offence under an enactment of Alberta or Canada.

Officer of the Legislature*: means the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner, or the Information and Privacy Commissioner.

order: is a direction or decision issued by the Commissioner to conclude an inquiry.

personal information*: means recorded information about an identifiable individual, including but not limited to:

- the individual's name, home or business address, or home or business telephone number;
- the individual's race, national or ethnic origin, colour, or religious or political beliefs, or associations;
- the individual's age, sex, marital status or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, blood type or inheritable characteristics;
- information about the individual's health and health care history, including information about a physical or mental disability;
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given;
- anyone else's opinion about the individual; and
- the individual's personal views or opinions, except if they are about someone else.

personal information bank*: is a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

prescribed*: means prescribed by regulation.

provincial public body: refers to a public body other than a local public body. This is not a term used in the *Act*, and is used in this publication only for convenience.

public body*: means:

- a department, branch or office of the Government of Alberta;
- an agency, board, commission, corporation, office or other body designated as a public body in the regulation;
- the office of a member of the Executive Council;
- the Executive Council Office;
- the Legislative Assembly Office;
- the office of the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner, or the Information and Privacy Commissioner; or
- a local public body;

but does not include:

- the office of the Speaker of the Legislative Assembly and the office of a Member of the Legislative Assembly; or
- the Court of Appeal of Alberta, the Court of Queen's Bench of Alberta, the Surrogate Court of Alberta or the Provincial Court of Alberta.

***quality assurance committee*:** is a committee that has as its purpose to study, assess and evaluate the provision of health services with a view to continuous improvement of the quality of health care or health services, or the level of skill, knowledge and competence of health service providers. This term applies only to quality assurance committees as defined in the *Alberta Evidence Act* and not to other quality assurance committees established within either health care bodies or other public bodies to monitor the quality of health services or other services.

***reasonable*:** involves a subjective assessment which can be deemed to be fair, proper, just, moderate, suitable under the circumstances, rational, governed by reason, not immoderate or excessive and to a standard to avoid liability for negligence, including the foreseeability of harm.

There are a variety of situations under the *Act* where reasonableness comes into play in assessments, decisions and duties for which public bodies are responsible, in particular:

- fulfilling the duty to assist applicants and to respond to requests without delay;
- assessing the amount of an invasion of privacy for an individual;
- assessing harm in exceptions;
- collecting, protecting, and assessing consistent uses and disclosures in relation to personal information;
- taking care to give a notice required under the *Act*; and
- determining appropriate severing of excepted information from a record.

***reasonably be expected to*:** in the context of the phrase "could reasonably be expected to" have a particular result means that there must be a clear cause and effect relationship between the disclosure and the expected result, and the likelihood of the result must be genuine and conceivable.

***record**:** is an inclusive term which means a record of information in any form and includes books, documents, maps, drawings, photographs, letters, vouchers and papers and *any* other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records.

***record of a credit union**:** for the purposes of the *Act*, means a record that originates from a credit union that is submitted to, or is received by, the Credit Union Deposit Guarantee Corporation.

records retention and disposition schedule: is a legal authority that describes the records under the control of a public body, specifies how long and where they must be kept as they progress through the phases of their life cycle, the format in which the records must be stored, and what their final disposition will be (destruction or archival preservation) at the end of their life cycle.

request: means a formal application under the *Act* for access to records or personal information in the custody or under the control of a public body.

review: is the examination by the Commissioner of:

- any decision, act or failure to act of the head of a public body that relates to an access request under the *Act*; or
- the collection, use or disclosure of personal information that is alleged to be non-compliant with **Part 2** of the *Act*.

scope: means the range of records covered by the legislation. The *Act* applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to certain records defined in **section 4(1)** of the *Act*. The scope of the legislation is dealt with in detail in Chapter 1 of this publication.

severing: means the physical removal, by masking or other means, of any information that is excepted from disclosure in order that the remainder may be disclosed.

third party*: means any person, group of persons or organization other than the person making a request or a public body. The term refers to a person, group of persons or organization whose information is in the custody or under the control of a public body and which may, therefore, be accessible under the *Act*.

time limit: means the time allowed for a response to be made or an action to be taken. The Alberta *Interpretation Act* stipulates that if a time is expressed to begin after or to be from a specified day, the time does not include that day; and if anything is to be done within a time after, from, of or before a specified day, the time does not include that day. The 30 day time limit for processing requests begins on the day after the request is received; the 20 day time limit for a third party response begins on the day after the third party notice is given; and an applicant has 60 days from the day after being notified of a decision to request a review of that decision by the Commissioner. Time limits refer to calendar days, not business days. If a time limit expires on a holiday, the limit is extended until the next day that is not a holiday.

trade secret: means information, including a formula, pattern, compilation, program, device, product, method, technique or process:

- that is used, or may be used, in business or for any commercial purpose;
- that derives independent economic value, actual or potential, from not being generally known to anyone who can obtain economic value from its disclosure or use;
- that is the subject of reasonable efforts to prevent it from becoming generally known; and
- the disclosure of which would result in significant harm or undue financial loss or gain.

transfer: is the act by which one public body formally passes to another public body responsibility for processing a request for access to, or correction of, records under the *Act*, usually because the receiving public body has a greater interest in the records.

transitory record: is a record containing information of a transient or ephemeral nature, and includes duplicate records, draft documents and working materials that do not have long-term value. Transitory records have no future administrative, financial, legal, research or historical value to the public body or the Government of Alberta. (See the Alberta Innovation and Science publication *A Guide to Identifying and Disposing of Transitory Records*.)

Appendix 2

Delegation Table

Appendix 2
Delegation Table

Responsibility / Description	Section Number	Retained By Head	Delegated to FOIP Coordinator	Other Delegated Authority *(title - specific or generic)*
Right of Access				
Abandonment of requests	7.1(1)			
Authority to grant continuing requests	8(2)			
Duty to assist applicants	9(1)			
Duty to create records	9(2)			
Authority to decide on content of response	11			
Authority to decide how access will be given	12			
Authority to extend time limit	13(1) & 13(3)			
Authority to request Commissioner's permission for extension	13(1) & 13(2)			
Authority to transfer a request	14 & 35.1			
Exceptions - Release and Refusal Decisions				
Business interests of a third party	15			
Personal privacy	16			

Responsibility / Description	**Section Number**	**Retained By Head**	**Delegated to FOIP Coordinator**	**Other Delegated Authority** *(title - specific or generic)*
Protection of individual or public health and safety	17			
Confidential evaluations	18			
Law enforcement	19			
Intergovernmental relations	20			
Cabinet confidences	21			
Local public body confidences	22			
Advice from officials	23			
Economic interests of a public body	24			
Testing procedures, tests and audits	25			
Privileged information	26(1) & (2)			
Conservation of heritage sites	27			
Information that is or will be available to public	28			
Third Party Intervention				
Giving third party notice	29			
Giving notice of decision	30			

Responsibility / Description	Section Number	Retained By Head	Delegated to FOIP Coordinator	Other Delegated Authority *(title - specific or generic)*
Giving other notices	16(2)(b) & 31			
Public Interest				
Approval of disclosure in public interest	31			
Collection, Protection and Retention of Personal Information				
Ensuring proper collection	33(3)			
Authority to decide on correction of personal information	35			
Ensuring protection of personal information	36			
Use and Disclosure of Personal Information				
Disclosure to relative of deceased individual	38(1)(aa)			
Disclosure when imminent danger to health or safety	38(1)(cc)			
Disclosure for research and statistical purposes and administration of agreements	40(c)			
Disclosure to guardian of a minor	79(1)(d)			
Reviews and Complaints				
Authority to ask the IPC for advice	52(1)			

Responsibility / Description	Section Number	Retained By Head	Delegated to FOIP Coordinator	Other Delegated Authority *(title - specific or generic)*
Authority to request IPC to disregard requests	53			
Require Commissioner to examine original record on site	54(4)			
Make representations to the Commissioner	66(3), 66(5) & 66(6)			
Asserting burden of proof	67			
Duty to comply with Commissioner's Order	68			
General Provisions				
Report uses or disclosures of personal information not in Directory	82(4)[*], 82(6)[**] & 82(8)			
Specify categories of records available without formal request	83			
Make manuals available	84			
Fees				
Authority to assess and collect fees	87			
Authority to waive fees	87(4)			

---

[*] Applies only to provincial government bodies.
[**] Applies only to local public bodies.

Appendix 3

Model Letters

Appendix 3
Model Letters

Introduction

The following sample letters are provided to assist public bodies in corresponding with applicants, third parties and others in the processing of access requests. The sample letters are intended to provide general guidance and may be altered to suit the circumstances of each request.

The letters are as follows:

A	Acknowledgment of Request
B	Notification during a Continuing Request
C	Transfer of Request
D	Notice Regarding Extension of Time Limit
E	Fee Estimate
E(1)	Abandonment of a Request
F	Response to Access Request – Granting Access
G	Response to Access Request – Denial of All or Part of Record(s)
H	Response to Access Request – Record Does Not Exist
I	Refusal to Confirm or Deny Existence of a Record
J	Letter to Speaker of the Legislative Assembly Regarding Parliamentary Privilege
K	Notice to Third Party under Section 29
L	Notice to Applicant under Section 29(4)
M	Notice to Third Party Regarding Decision under Section 30
N	Notice to Applicant Regarding Decision under Section 30
O	Notice to Third Party under Section 31 (Disclosure in the Public Interest)
P	Notice to Third Party under Section 31 after Disclosure of Information
Q	Notice to Third Party under Section 16(4)(b)
R	Acknowledgment of Receipt of Correction Request
S	Notification Concerning a Request for Correction or Annotation
T	Notice to Public Bodies in Receipt of Personal Information
U	Initial Letter to Expert under Section 17(2)
V	Letter Transmitting Records to Experts under Section 17(2)

Model Letter A – Acknowledgment of Request

Purpose: *To acknowledge receipt of the applicant's request for information, to ask for clarification of a request and/or to request that initial fees be paid in order that the request may be considered complete and processing can commence.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

Your request for access to [*describe the information requested*] under the *Freedom of Information and Protection of Privacy Act* (the *Act*) was received by [*public body*] on [*date*].

Option A.1: General Acknowledgment

We will provide the information available to you under the *Act* as quickly as possible. Although the *Act* allows us a maximum of 30 days to respond, we will reply sooner than [*date*], if possible.

Option A.2: Need to Supply More Details

Unfortunately, your request for access to information does not provide sufficient specific details to identify the records you may be requesting. [*Name of public body*] cannot begin to process your request until we receive additional information to help us [*identify the record or make the request more specific*]. Please help us to clarify your request by supplying any of the following details of which you are aware:

[*list details you are requesting*]

Model Letter A – Acknowledgment of Request (continued)

Option A.3: Failure to Include Initial Fee

Unfortunately, you did not include the initial fee of $25.00. The *Act* allows us 30 days to respond to your request, but this time period will not commence until the initial fee has been received. Please forward the fee to [*appropriate address within the public body*] as quickly as possible.

The processing of the request will commence immediately upon the receipt of your fee.

Option A.4: Acceptance of Continuing Request

We note that you wish your request to have continuing status under section 8 of the *Act*. [*Name of public body*] is granting the request continuing status, and a schedule indicating the period of the request and on what dates the continuing request will be deemed to be received and activated is attached. You will be notified on each of these dates that the request process has begun and when a response can be anticipated.

If you find this schedule unsatisfactory, please write to me or call me at [*telephone number*].

Option A.5: Rejection of Continuing Request

We note that you wish your request to have continuing status under section 8 of the *Act*. [*Name of public body*] does not grant your request [*state reasons*]. For these reasons, we will only respond to this request as a single access request for records that currently exist.

Option A.6: Clarification of Request

We have now had an opportunity to discuss your request with you [*state method and date*]. We agreed that the request would now focus on [*describe the subject and/or the information agreed upon*]. If this understanding is not correct, please contact me at [*telephone #*] as soon as possible. This letter serves as a notice that it is this request which [*name of public body*] is proceeding to process. We will provide the information available to you under the *Act* as quickly as possible. Although the *Act* allows us a maximum of 30 days to respond, we will reply sooner than [*date*], if possible.
Section 62 of the *Freedom of Information and Protection of Privacy Act* provides that you may make a written request to the Information and Privacy Commissioner to review this matter. You have 60 days from the date of this notice to request a review by writing to the Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

Model Letter A – Acknowledgment of Request (continued)

When requesting a review, please provide the Office of the Commissioner with the following information:

1. The reference number noted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request form that you sent to [*name of public body*].

If you have any questions, please write to me or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter B – Notification During A Continuing Request

Purpose:	*To notify a requester who has made a continuing request that work has begun on processing records at a particular date set out in the schedule required by section 8 of the Act.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

Option B.1: No Fee Required

[*Name of public body*] is commencing to process your continuing request concerning [*set out general subject*] in accordance with the established schedule. The processing, due to commence on [*date*], is now under way. We will make every effort to provide the information requested as quickly as possible and no later than [*date*].

Option B.2: Deposit Required

As indicated in the letter of [*date of original fee estimate for the continuing request*], [*name of public body*] will process your continuing request concerning [*set out general subject*] in accordance with the schedule established, when the deposit for this scheduled instalment of the request is received. Please forward the deposit of [*$ amount*] made payable to [*the Provincial Treasurer or appropriate officer of public body*]. This reply must be sent to [*name of officer, office and address of public body*] and should quote the reference number provided at the top of this letter. When we have received your deposit, processing of your request will proceed.

If you have any questions now or during the processing of this portion of your request, please write or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter C – Transfer of Request

Purpose:	*To advise an applicant that his or her access request or request for correction of personal information has been transferred.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

Your request for [*information or correction of your personal information*] has been forwarded to [*name of public body, address and telephone number*] and this body has agreed to process it. Your request was transferred on [*date*] under [*section 14 or 35.1*] of the *Freedom of Information and Protection of Privacy Act* because [*name of public body*] [*explain the reason for the transfer; i.e., the record was produced by or for the other public body or the other public body was the first to obtain the record, or the record is in the custody or under the control of the other public body*].

[*Name of the other public body*] will respond to you before [*date – 30 days from the date the other public body received the transferred request*] unless it extends the time limit for responding to you under section 13. [*Name of FOIP Coordinator*] at [*public body*] will contact you shortly to acknowledge receipt of this request.

If you have any questions, please write to me or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

cc: [*Other public body contact*]

Model Letter D – Notice Regarding Extension of Time Limit

Purpose: *To advise an applicant of a time extension taken to process a request.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

[*Name of public body*] received your request for access to information on [*date*].

Normally, [*name of public body*] responds to a request for information within 30 days after receiving the request. However, in limited circumstances, the *Freedom of Information and Protection of Privacy Act* provides that a public body may extend this time limit.

Option D.1: Time Extension to Clarify Request

In this case, there is a need for us to obtain more information from you before we can identify the records that deal with the subject of your request. We will need a time extension of [*number of days*] to do this and identify the applicable records.

Option D.2: Consultation with Third Party or Parties or Other Public Body or Bodies

A preliminary review of the records you have requested indicates that extensive consultations with other parties including [*name of third party or parties or public body or bodies*] may be required before we can fully process your request. This consultation is necessary for us to deal completely with the records that are the subject of your request. We will require a time extension of [*number of days*] to carry out this process.

Option D.3: Large Number of Records

Your request involves a large number of records. The volume of information involved cannot be processed within the usual 30-day limit. An extension of time of [*number of days*] will allow [*name of public body*] to provide you with a complete response to your request.

Model Letter D – Notice Regarding Extension of Time Limit (continued)

Option D.4: Multiple concurrent requests

[*You or you and others working for the same organization or working in association with you*] have made multiple concurrent requests. We have consulted with the Information and Privacy Commissioner about the difficulties this causes in terms of responding to all requests within the 30-day time limit in the *Act*. The Commissioner has given us permission to extend the time for responding by [*number of days*].

[*Conclusion for all options*]

A response to your request will be ready no later than [*proposed date*]. We will try to respond sooner, if possible.

If you have any questions regarding this time extension, please contact [*name and job title*] at [*business address*] or telephone [*number*].

If you feel this time extension is unjustified, section 62 of the *Freedom of Information and Protection of Privacy Act* provides that you may ask the Information and Privacy Commissioner to review this decision. You have 60 days from the date of this notice to request a review by writing to the Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

When requesting a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of public body*].

If you have any questions, please write or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter E – Fee Estimate

Purpose: To advise an applicant of the amount of fees that will be involved in processing a request.

[*Reference number*]

[*Date*]
[*Applicant's name and address*]

Dear [*applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

[*Name of public body*] received your request for access to information on [*date*]. Section 87 of the *Freedom of Information and Protection of Privacy Act* provides that fees may be charged for providing you with the information which you requested.

Fees, over and above the initial fee paid at the time you made the request, are assessed because [*provide rationale for fees being assessed*].

The fee for providing the records you have requested is estimated to be [*$ amount*]. We have calculated this amount as follows:

[*provide calculation*]

Option E.1: Deposit

Please reply to us in writing within 20 days of the date of this notice indicating that you accept this estimate and enclose a deposit of [*$ amount*] made payable to [*the Provincial Treasurer or appropriate officer of public body*]. This reply must be sent to [*name of officer, office and address of public body*] and should quote the reference number provided at the top of this letter. When we have received your response and deposit, processing of your request will continue.

Option E.2: No Deposit

Please reply to us in writing within 20 days of the date of this notice indicating that you accept this estimate and will pay these fees when requested to do so. Please send the reply to [*name of officer, offices and address of public body*] and quote the reference number provided at the top of this letter. When we have received your response, processing of your request will continue.

Model Letter E – Fee Estimate (continued)

Option E.3: Refusal of Fee Waiver

Your request for a fee waiver cannot be granted [*state reason*]. Please reply to us in writing within 20 days of the date of this notice indicating that you accept this estimate and enclose a deposit of [*specify amount*]. Please send the reply to [*name of officer, offices and address of public body*] and quote the reference number provided at the top of this letter. When we have received your response, your request will be processed.

If you find the fees a burden to you, we would be pleased to discuss approaches to processing the request which may reduce the fees and still provide the information you require. Please write or call [*name, title, address and telephone number*], who may be able to assist you.

[*For options E.1 and E.2*]

Section 87(4) provides some limited situations where fees can be reduced, or waived entirely, if you cannot afford to pay or there are other reasons that justify excusing the fee, or if the record relates to a matter of public interest. If you believe that one of these circumstances applies to you, you should raise it with the officer mentioned above.

[*Conclusion for all options*]

Section 62 of the legislation allows you may ask the Information and Privacy Commissioner to review this fee estimate and any decision made on a request for a fee waiver. The *Act* allows you 60 days from the date you receive this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

When requesting a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of public body*].

If you have any questions, please write or call the officer named above or myself at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter E(1) – Abandonment of Request

Purpose:	*To inform the applicant that his or her request is going to be considered abandoned under section 7.1.*
Note:	*The time line to allow the applicant to reactivate the request within 12 months is a suggested guideline, not a requirement of the Act. Public bodies may choose to alter this according to the nature of the request or the records involved.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

Option E(1).1: Abandonment Indicated

You indicated to us on [*date*] that you were abandoning your request [*reference number and subject*]. If you wish to reactivate your request at any time up to [*date 12 months from the date of closure*], you may do so without making another request or submitting an initial fee. After that date, you will have to submit another request and any initial fee that may be required

Option E(1).2: Abandonment Not Indicated

We have not received any communication concerning your request since [*date of letter seeking further information or requesting fee*]. For this reason, we are closing the file on your request [*reference number and subject*]. If you wish to reactivate your request at any time up to [*date 12 months from the date of closure*], you may do so without making another request or submitting an initial fee. After that date, you will have to submit another request and any initial fee that may be required.

If you disagree with this decision, section 62 of the *Freedom of Information and Protection of Privacy Act* provides that you may ask the Information and Privacy Commissioner to review this decision. You have 60 days from the date of this notice to request a review by writing to the Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

Model Letter E(1) – Abandonment of Request (continued)

When requesting a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of public body*].

If you have any questions, please write or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter F – Response to Access Request – Granting Access

Purpose: To inform an applicant that access will be granted.

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request Under Consideration*]

I am responding to your request of [*date*] for access to information. We are pleased to provide access to [*specify subject and records generally*].

Option F.1: Copy Enclosed

A copy of the record is enclosed.

Option F.2: Applicant to View Originals

You have requested an opportunity to examine the original records rather than receive copies of them. We invite you to examine the record(s) at [*place and address*] on [*date*] at [*time*]. If you are unable to examine the records at that time, please contact [*name and telephone number*] to make alternate arrangements.

Option F.3: Records Cannot be Copied

The record(s) you have requested cannot be copied because [*provide reason*]. We invite you to examine the original record(s) at [*place and address*] on [*date*] at [*time*]. If you are unable to examine the record(s) at that time, please contact [*name and telephone number*] to make alternate arrangements.

Option F.4: Fees Required

As we informed you in our fee estimate of [*date*], your request has now been processed and fees totaling [*$ amount and calculation, if previous deposit received*] must be paid before access can be provided.

Model Letter F – Response to Access Request – Granting Access (continued)

Please make your cheque or money order payable to [*Provincial Treasurer or local public body*] and send it to [*name of officer, office and address of public body*].

If you feel that your request has not been answered completely or that you require further clarification, please contact [*name and job title*] at [*business address and telephone number*].

Under section 62 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review the assessment of a fee or any other matter concerning this response to your request. You have 60 days from the date of this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

If you wish to request a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of public body*].

If you have any questions, please write or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter G – Response to Access Request – Denial of All or Part of Record*(s)*

Purpose:	*To inform an applicant that access to all or part of the records requested has been denied.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

I am replying to your request of [*date*] for access to [*general subject of records*].

Option G.1: Total Denial

Unfortunately, access to all the information that you requested is denied under section(s) [*put in an explanation, including the detailed sections on which denial is based*].

Option G.2: Some Records Available

I am pleased to inform you that access is being provided to [*specify particular records*].

- A copy of the record(s) is attached; or
- You requested to examine the original records rather than receive copies. We invite you to examine the record(s) at [*place and address*] on [*date*] at [*time*]. If you are unable to examine the records at that time, please contact this office to make alternative arrangements; or
- The record(s) to which you are being given access cannot be copied. We invite you to examine the original record(s) at [*place and address*] on [*date*] at [*time*]. If you are unable to examine the record(s) at that time, please contact this office to make alternative arrangements.

Access to all other records has been denied under section(s) [*give precise references*] of the *Freedom to Information and Protection of Privacy Act.*

Model Letter G – Response to Access Request – Denial of All or Part of Record(s) (continued)

Option G.3: Severed Information

Some of the records you requested contain information that is excepted from disclosure under *the Freedom of Information and Protection of Privacy Act*. We have severed the excepted information so that we could disclose to you the remaining information in the records.

The severed information is excepted from disclosure under sections [*provide section numbers and descriptors*] of the *Act*. The detailed sections supporting the excising of particular information is [*provided in the attached list or indicated on the face of each record*].

Under section 62 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review the decision not to disclose information that you requested. You have 60 days from the receipt of this notice to request a review by writing the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

Option G.4: Excluded Records

The following records which you requested [*describe records*] are excluded from the coverage of the *Freedom of Information and Protection of Privacy Act* under section [*provide paragraph of section 4*].

We are not disclosing these records to you.

OR

We are disclosing (all or part of the particular records) outside the provisions of the *Freedom of Information and Protection of Privacy Act* and a copy of these is enclosed.

[***If fees are to be charged, reference should be made to the options for additional wording in Model Letter F.***]

Under section 62 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review the decision that the records that you requested are excluded from the scope of the *Act*. You have 60 days from the receipt of this notice to request a review by writing the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

If you wish to request a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.

3. A copy of your original request for information that you sent to [*name of public body*].

If you have any questions about this letter, please write or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter H – Response to Access Request – Record Does Not Exist

Purpose: To advise an applicant that a record does not exist.

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

I am writing about your request of [*date*] for access to information under the *Freedom of Information and Protection of Privacy Act*.

I regret to inform you that a search by [*name of public body*] has failed to retrieve any records relating to the subject of your request. [*Outline all steps taken to locate records and, if the records have been destroyed, provide information, if possible, as to when and under what authority this was done.*]

Under section 62 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review the finding that records pertinent to the request [*could not be located or have been destroyed*]. You have 60 days from the date of this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

If you wish to request a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of public body*].

If you have any questions about this letter, please write or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter I – Refusal to Confirm or Deny Existence of a Record

Purpose: To respond to an applicant where it is necessary to "neither confirm or deny" the existence of a record.

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

I am writing about your request of [*date*] for access to information concerning [*specify subject*].

We are unable to confirm or deny the existence of the record(s) you have requested. However, if such information did exist, it would be excepted from disclosure under sections [*specify sections and descriptors*] of the *Freedom of Information and Protection of Privacy Act*.

Under section 62 of that *Act*, you may ask the Information and Privacy Commissioner to review this decision. You have 60 days from the date of this notice to ask for a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

If you wish to request a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of public body*].

If you have any questions about this decision, please write or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter J – Letter to Speaker of the Legislative Assembly Regarding Parliamentary Privilege

Purpose: *To obtain a determination from the Speaker of the Legislative Assembly as to whether or not records contain information subject to parliamentary privilege.*

[*Reference number*]

[*Date*]

[*Speaker's name and address*]

Dear [*Name of Speaker*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

[*Name of public body*] has received a request under the *Freedom of Information and Protection of Privacy Act*. The request is for records concerning [*subject of request*] and we believe that the records attached to this letter may contain information which is subject to parliamentary privilege under section 26(1) of the *Act*.

Your assistance in making a determination, as required under section 26(3) of the legislation, as to whether or not parliamentary privilege applies in this case would be appreciated. We received the request on [*date*] and must respond to the applicant by [*date*]. Your prompt attention to this matter would also be most appreciated.

If you have any questions regarding the records or the request do not hesitate to call me at [*telephone number*].

Sincerely,

[*Head of public body*]
[*Title*]

Attachment

Model Letter K – Notice to Third Party under Section 29

Purpose: *To advise a third party that an applicant has requested access to information that affects their business interests or personal privacy.*

[*Reference number*]

[*Date*]

[*Third party's name and address*]

Dear [*Third party's name*]:

Re*:* Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

[*Name of public body*] has received a request under the *Freedom of Information and Protection of Privacy Act* (the *Act*) to disclose [*describe the records as they relate to the third party*]. A copy of the information that pertains to you accompanies this letter [*include a copy of the record whenever possible without disclosing information that is excepted under the Act*].

[*Make a note of the portion of the record that is being considered for severing, if that is the case.*]

We would appreciate receiving your views regarding disclosure of this information.

Option K.1: Business Interests (section 15)

As section 15 of the *Act* indicates, [*name of the public body*] must disclose information to the applicant unless:

1. the records contain certain types of information as described on the attached sheet; and
2. the information was supplied in confidence; and
3. the disclosure of the information could reasonably be expected to result in one or more of the harms specified on the attached sheet.

A public body must refuse to disclose information that was collected on a tax return, or collected for the purposes of determining tax liability or in collecting a tax.

A copy of section 15 of the *Act* is attached to this letter to assist you. After reviewing the material, please provide your views on the disclosure of the records in writing to [*me, or name and job title*] by [*date*]. You have 20 days in which to respond to this notice. You

Model Letter K – Notice to Third Party under Section 29 *(continued)*

may either: (1) consent to the disclosure of the information; or, (2) make written representations explaining why the information should not be disclosed.

If you wish to have any of the information pertaining to your business withheld, it is important that you provide clear and specific reasons which focus on the type of harm that may result as specified in section 15 of the *Act*.

Your input and other relevant factors will be considered when deciding whether to disclose the requested information. Please note that, if we do not receive written representations from you by [*date*], we are required under the *Act* to make a decision based on the information that we have available. I will write to you by [*date*] to inform you of [*public body's*] decision.

Option K.2: Personal Privacy (section 16)

As section 16 of the *Act* (attached) indicates, [*name of the public body*] is required to withhold personal information if it is determined that disclosure would be an unreasonable invasion of a third party's personal privacy.

Because disclosure of the requested records might be an unreasonable invasion of your personal privacy, your input would be valuable in helping us decide whether to disclose them.

You have 20 days from the date on this notice to respond. After reviewing the accompanying material, please write to [*me, or name and job title*] by [*date*] indicating whether you consent to the disclosure of the information or explaining why you feel the information should be withheld.

Your input and other relevant factors will be considered when deciding whether to disclose the requested information. Please note that, if we do not receive written representations from you by [*date*], we are required under the *Act* to make a decision based on the information that we have available. I will write to you by [*date*] to inform you of [*public body's*] decision.

For further information concerning your rights and responsibilities under the *Freedom of Information and Protection of Privacy Act*, please refer to the accompanying *Explanatory Notes* [*either Third Party Notice re: Business Interests, or Third Party Notice re: Personal Information*].

If you have any questions, please write to me or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter K – Notice to Third Party under Section 29 *(continued)*

Explanatory Note

Notice under Section 15
Third Party Business Interests

The *Freedom of Information and Protection of Privacy Act* provides a right of access to records held by public bodies.

We have received a request for access to records in which you have an interest. We are required to provide access to as much of the requested records as possible. We may withhold only the information covered specifically in the *Act*'s exceptions.

We are notifying you in order to give you an opportunity to express any concerns that you may have about disclosure of the records. To be excepted from disclosure, the third party business information must meet ***all three*** of the criteria in section 15 of the *Act*, harm to the business interests of a third party.

These criteria are:

1. The information is a trade secret or commercial, financial, labour relations, scientific or technical information of a third party.

2. The information was supplied, implicitly or explicitly, in confidence. There must be evidence that the information has been consistently treated in a confidential manner.

3. One or more of the following harms will occur if the information is disclosed. The disclosure of the information will:

    - harm significantly the competitive position or interfere significantly with the contractual or other negotiations of the third party;

    - result in similar information no longer being supplied to the public body where it is in the public interest that similar information continues to be supplied. This does not apply where a statute or regulation requires that the information be supplied;

    - result in undue financial loss or gain to any person or organization; or

    - reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer, or other person or body appointed to resolve or inquire into a labour dispute.

Model Letter K – Notice to Third Party under Section 29 *(continued)*

Explanatory Note *(continued)*

Notice under Section 15
Third Party Business Interests

A public body must refuse to disclose any information about a third party that was collected on a tax return or collected for the purpose of determining tax liability or collecting a tax.

You have two options:

1. You may consent in writing to the disclosure of all or some of the information; or

2. If you feel that the provisions in section 15 apply to some or all of the information in the requested records, you may make written representations to us. Your representations should be directed only to information you would like to have excepted from disclosure. It must provide detailed evidence to support your claim for the exception. Please mark the exact portions of the records you wish to have withheld.

Your representation will be one of the factors that we consider in deciding whether or not to disclose all or part of the records. If we decide to disclose all or part of the records, you will be notified beforehand. If you disagree with the decision, you may ask the Information and Privacy Commissioner to review the decision.

For further information, please contact [*name of coordinator, name of public body, address, telephone and fax numbers*].

Model Letter K – Notice to Third Party under Section 29 *(continued)*

Explanatory Note

Third Party Notice under Section 16
Protection of Personal Privacy

The *Freedom of Information and Protection of Personal Privacy Act* balances the public's right of access to records with the need to protect the privacy of individuals whose personal information is held by public bodies.

We have received a request under the *Act* by another person or organization for access to your personal information. We are notifying you in order to give you an opportunity to express any concerns that you may have regarding the disclosure of the personal information.

You have two options:

1. You may consent in writing to the disclosure of some or all of the information; or
2. You may make tell us, in writing, your concerns about the disclosure of the information, and explain why it would be an unjustified invasion of your privacy.

We will consider your representation in deciding whether or not to disclose the requested personal information. If it is decided that some or all of the information is to be disclosed, we will notify you before this takes place. If you disagree with that decision, you may ask the Information and Privacy Commissioner to review the decision.

For further information, please contact [*name of coordinator, name of public body, address, telephone and fax numbers*].

Model Letter L – Notice to Applicant under Section 29(4)

Purpose: *To advise an applicant that a third party will be consulted about disclosure of the requested information.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

On [*date*], I received your request for access to records held by [*name of public body*].

The requested records contain information which, if disclosed, may affect the interests of another person or organization. We have contacted the affected party, as required under section 29 of the *Act*, to provide them with an opportunity to consent to disclosure or to make representations explaining as to why disclosure would be [*an unreasonable invasion of their personal privacy or may harm their business interests*]. We will notify you of our decision regarding your request by [*date*].

If you have any questions, please write to me or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter M – Notice to Third Party Regarding Decision under Section 30

Purpose: To advise a third party of decision on disclosure.

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

Option M.1: Third Party Representations Received, Objecting to Disclosures; Public Body Decides to Refuse Access to the Records

Thank you for your views on the disclosure of [*describe requested records as they relate to the third party*].

After considering your representations in favour of refusing disclosure of these records, [*name of public body*] has decided to refuse the applicant's access request. This decision is based on [*insert specific sections of the Act and the reasons those sections apply*].

Upon notification of our decision, the applicant has 60 days to ask for a review by the Information and Privacy Commissioner. If that happens, the Commissioner may contact you as an interested party.

Option M.2: Third Party Representations Received, Objecting to Disclosures; Public Body Decides to Give Access to All or Part of the Records

Thank you for your views on the disclosure of [*describe requested records as they relate to the third party*].

After considering your representations in favour of refusing disclosure of these records and other relevant factors, [*name of public body*] has decided to give the applicant access [*or partial access*] to the records. [*If partial access, describe the parts of the records that will be disclosed and the parts that will be withheld. Provide copies or insert specific sections of the Act under which information will be withheld, and the reasons the sections apply. If full access, insert explanation of why sections 15 or 16 do not apply to the*

Model Letter M – Notice to Third Party Regarding Decision under Section 30 (continued)

information that was the subject of the third party's representations.] This decision is based on [*insert specific sections of the Act and the reasons those sections apply*].

You may ask the Information and Privacy Commissioner to review the decision to disclose these records. You have 20 days from the date of this notice to request a review by writing the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

If no request for a review is made within 20 days, the applicant will be given access to the records.

Option M.3: Third Party Consented to Disclosure of Information; Public Body Decides to Refuse Access to the Records Because Another Exception Applies

Thank you for your views on the disclosure of [*describe requested records as they relate to the third party*].

After considering all the relevant factors, [*name of public body*] has decided to refuse the applicant access to these records. The decision is based on [*insert specific sections of the Act under which information will be withheld, and the reasons the sections apply.* ***Note that information cannot be withheld under sections 15 or 16 if the third party that is involved has consented to disclosure; however, another exception may apply.***]

This decision was made by [*name and job title*].

Upon receipt of the response to this request, the applicant has 60 days to ask the Information and Privacy Commissioner to review this decision.

Option M.4: Third Party Consented to Disclosure; Public Body Decides to Give Access to All or Part of the Records

Thank you for your views on the disclosure of [*describe requested records as they relate to the third party*].

[*Name of public body*] has decided to give the applicant access [*or partial access*] to these records. [*If partial access, provide copies or describe the parts of the records that will be disclosed and the parts that will be withheld. Insert specific sections of the Act under which information will be withheld, and the reasons those sections apply.* ***Information cannot be withheld under sections 15 or 16 if the affected third party has consented to disclosure. However, another exception may apply.***]

This decision was made by [*name and job title*].

Model Letter M – Notice to Third Party Regarding Decision under Section 30 (continued)

[*Insert this paragraph if the applicant will be given partial access.*] After receiving these records, the applicant has 60 days to ask for a review by the Information and Privacy Commissioner.

Option M.5: No Response Received from Third Party; Public Body Decides to Refuse Access to the Records

We have not received your reply to our letter of [*date of third party notice*] which requested your views on disclosure of [*describe records as they relate to the third party*]. [*Name of the public body*] has decided to refuse the applicant access to these records. This decision is based on [*insert specific sections of the Act and the reasons those sections apply*].

This decision was made by [*name and job title*].

The applicant has 60 days to ask the Information and Privacy Commissioner to review this decision. If that happens, the Commissioner may contact you as an interested party.

Option M.6: No Response Received from Third Party; Public Body Decides to Give Access to All or Part of the Records

We have not received your reply to our letter of [*date of third party notice*] which requested your views on disclosure of [*describe records as they relate to the third party*]. [*Name of the public body*] has decided to give the applicant access [*or partial access*] to these records. [*If partial access, provide a copy or describe the parts of the records that will be disclosed and the parts that will be withheld. Insert specific sections of the Act under which information will be withheld, and the reasons those sections apply.*]

This decision was made by [*name and job title*].

Under Section 62 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review the decision to disclose these records. You have 20 days from the date of this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

If no request for review is made within 20 days, we will give the applicant access to the records.

Model Letter M – Notice to Third Party Regarding Decision under Section 30 (continued)

[*Insert the following paragraph if applicant will be given partial access.*] The applicant has the right to ask the Information and Privacy Commissioner to review the decision to deny access to a part of the records. If you have any questions, please write to me or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter N – Notice to Applicant Regarding Decision under Section 30

Purpose: *To advise an applicant of a decision regarding disclosure under the third party notification process.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request under Consideration*]

Option N.1: Third Party Representations Received Objecting to Disclosure and Public Body Decides to Refuse Access to the Records

We have reached a decision about your request of [*date*] for access under the *Freedom of Information and Protection of Privacy Act* to [*briefly state subject of records requested*].

After considering all relevant factors, including representations received from the third party [*third parties*] whose interests could be affected by the disclosure of the records, we have refused access to the requested records based on [*insert specific sections of the Act and the reasons those sections apply*].

This decision was made by [*name and job title*].

Under section 62 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review this decision. You have 60 days from the date of this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

If you wish to request a review, please provide the Commissioner's office with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.

Model Letter N – Notice to Applicant Regarding Decision under Section 30 (continued)

3. A copy of your original request for information that you sent to [*name of public body*].

Option N.2: Third Party Representations Received Objecting to Disclosure or No Response Received from Third Party and Public Body Decides to Give Access to All or Part of the Record(s)

I am writing about your request of [*date*] for access under the *Freedom of Information and Protection of Privacy Act* dealing with [*subject of record(s)*].

We have notified the affected third party [*third parties*] and have given that party [*those parties*] an opportunity to make representations. [*Name of public body*] has decided to give access [*or partial access*] to the records you requested.

[*If applicable*] You should be aware that you will be required to pay [*$00.00*] in fees before final access may be provided.

This decision was made by [*name and job title*].

The third party has 20 days to request that the Information and Privacy Commissioner review this decision. If the third party does not request the Commissioner to review this decision, we will give you access to the records on [*date*].

[*For full access, insert the details of providing access.*]

[*For partial access, describe the parts of the records that will be disclosed and the parts that will be withheld. Insert specific sections of the Act under which information will be withheld, and the reasons those sections apply. Provide access details.*]

Under section 62 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review any aspect of this decision. You have 60 days from the date of this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

If you wish to request a review, please provide the Commissioner's office with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of public body*].

Model Letter N – Notice to Applicant Regarding Decision under Section 30 (continued)

Option N.3: Third Party Consents to Disclosure of Information and the Public Body Decides to Give Access to All or Part of the Records

I am writing about your request of [*date*] for access under the *Freedom of Information and Protection of Privacy Act* to [*subject of records*].

The affected third party has consented to the disclosure of the information. I am pleased to advise you that [*name of public body*] has decided to provide access [*or partial access*] to the records you requested.

The decision was made by [*name and job title*].

[*For full access, provide details of giving access.*]

[*For partial access, describe the parts of the records that will be disclosed and the parts that will be withheld. Insert specific sections of the Act under which information will be withheld, and the reasons those sections apply.* ***Information cannot be withheld under sections 15 and 16 if the affected third party has consented to disclosure. However, another exception may apply.*** *Also provide access details.*]

Under section 62 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review any decision to deny access to a part of these records. You have 60 days from the date of this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

If you wish to request a review, please provide the Commissioner's office with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of public body*].

Option N.4: Third Party Consented to Disclosure of Information But Public Body Decides to Refuse Access to the Records Under Another Exception

I am writing about your request of [*date*] for access under the *Freedom of Information and Protection of Privacy Act* to [*subject of record(s)*].

Model Letter N – Notice to Applicant Regarding Decision Under Section 30 (continued)

The affected third party has consented to the disclosure of the information. However, access to the requested record(s) is refused based on [*insert specific sections of the Act and the reasons those sections apply*].

This decision was made by [*name and job title*].

Under section 62 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review this decision to deny access to the record(s). You have 60 days from the date of this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

If you wish to request a review, please provide the Commissioner's office with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of public body*].

If you have any questions, please write to me or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter O – Notice to Third Party under Section 31 (Disclosure in the Public Interest)

Purpose: *To give a third party notice, before the fact, that information concerning the party will be disclosed through use of the public interest override.*

[*Reference number*]

[*Date*]

[*Third party's name and address*]

Dear [*Third party's name*]:

Re: Disclosure of Information in the Public Interest

Section 31 of the *Freedom of Information and Protection of Privacy Act* requires a public body to disclose information:

1. about a risk of significant harm to the environment, to the health or safety of the public, a group of people or an individual; or
2. the disclosure of which is, for any other reason, clearly in the public interest.

In accordance with this requirement, [*name of public body*] intends to disclose information that relates to you, in the public interest. [*Describe how the information relates to the third party. Explain why section 31 applies to the records in question. Provide a copy of the record if a record exists.*]

We would appreciate receiving your views regarding disclosure of these records. Because of the urgency of the circumstances, I ask that you contact me [*address, telephone and fax numbers*] by [*date and time*] if you wish to make representations explaining why the records should not be disclosed.

Sincerely,

[*Name*]
[*Title*]

Attachment

Model Letter P – Notice to Third Party under Section 31 after Disclosure of Information

Purpose: *To advise a third party, after the fact, that information concerning the party has been disclosed under the public interest provision.*

[*Reference number*]

[*Date*]

[*Third party's name and address*]

Dear [*Third party's name*]:

Notice of Disclosure of Information under the
***Freedom of Information and Protection of Privacy Act*, section 31(4)**

[*Name of public body*] has disclosed information that relates to you in compliance with the requirements of section 31 of the *Freedom of Information and Protection of Privacy Act*. This *Act* requires a public body to disclose information:

1. about a risk of significant harm to the environment, to the health or safety of the public, a group of people, or an individual; or

2. the disclosure of which is, for any other reason, clearly in the public interest.

The information disclosed is [*explain the information, provide a copy of the record if a record exists, and explain why section 31 applies to the information*]. This decision was made by [*name and job title*].

Sincerely,

[*Name*]
[*Title*]

Attachment

cc: Information and Privacy Commissioner

Model Letter Q – Notice to Third Party under Section 16(2)(b)

Purpose: To advise a third party of disclosure of records under section 16(4)(b).

[*Reference number*]

[*Date*]

[*Third party's name and address*]

Dear [*Third party's name*]:

Re: Disclosure of Information for Health or Safety

[*Name of public body*] has disclosed the following records in response to a request under the *Freedom of Information and Protection of Privacy Act*. These records contain information that may affect your interests. [*Describe records as they relate to the third party.*]

Section 16(2)(b) of the *Act* allows a public body to disclose information if there are compelling circumstances affecting anyone's health or safety.

In accordance with this requirement, [*name of public body*] has disclosed the records for the following reason(s):

[*Explain how section 16(2)(b) applies to the records in question.*]

This decision was made by [*name and job title*].

Under section 62 of the *Freedom of Information and Protection of Privacy Act*, you may ask the Information and Privacy Commissioner to review the decision to disclose these records. You have 60 days after the date of this notice to make a written request for review to the Commissioner's office at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

If you have any questions, please write to me or call at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter R – Acknowledgment of Receipt of Correction Request

Purpose: To acknowledge receipt of the applicant's request to correct his or her personal information.

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request for Correction under Consideration*]

Your request for correction of your personal information under the *Freedom of Information and Protection of Privacy Act* [the *Act*] was received by [*name of public body*] on [*date*].

We will respond to your request by [*date*], or sooner if possible.

If you have any questions, please write to me or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter S – Notification Concerning a Request for Correction or Annotation

Purpose: *To advise an individual whether or not a request for correction has been agreed to and, where it has not, that the record has been annotated.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Freedom of Information and Protection of Privacy Act
[*Request for Correction under Consideration*]

Option S.1: Correction Agreed To

Your request for a correction of [*error or omission*] has been agreed to by [*name of public body*] and your record has been corrected as you requested.

A copy of your new record incorporating the correction accompanies this notice [*or you can inspect the corrected record at – name and address of appropriate office*].

Option S.2: Correction Refused

Your request for a correction of [*error or omission*] has been refused by [*name of public body*], but [*your record has been annotated recording the correction that you requested and the fact that it was not made OR the correction that you requested and the fact that it was not made has been linked to your record*]. A copy of the completed form used to make the annotation is included with this notice. If you wish additional information to be included in the annotation, please provide it to us in writing.

The following public bodies, [*name public bodies*], to which the information has been disclosed over the last year have been informed of the facts of [*the correction or annotation*] and requested to amend their files to reflect this information.

Model Letter S – Notification Concerning a Request for Correction or Annotation (continued)

[*In the case of refusal*] You may request the Information and Privacy Commissioner to review our decision to refuse to correct your personal information. The *Act* allows you 60 days from the date you receive this notice to request a review by writing to the Information and Privacy Commissioner at 410, 9925 – 109 Street, Edmonton, Alberta, T5K 2J8.

If you wish to request a review, please provide the Office of the Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for correction which you sent to [*name of public body*].

If you have any questions, please write to me or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter T – Notice to Public Bodies in Receipt of Personal Information

Purpose: *To advise public bodies which have received personal information that a correction or annotation has been made.*

[*Reference number*]

[*Date*]

[*Name of public body*]

Dear [*Name of official*]:

On [*date*], [*name of originating public body*] disclosed to you information concerning [*name of person requesting correction*]. This information has [*been corrected and a copy of the corrected record is attached or annotated in the following way to reflect a correction requested but not made*]. Section 35(3) of the *Freedom of Information and Protection of Privacy Act* requires that we notify you of this correction. Please amend your records or link the correction or annotation to them in order to ensure that they contain this new information.

Sincerely,

[*Name*]
[*Title*]

Model Letter U – Initial Letter to Expert under Section 17(2)

Purpose: *To establish conditions for the disclosure of personal information to an expert under section 17(2).*

[*Reference number*]

[*Date*]

[*Name and address of expert*]

Dear [*Name of expert*]:

Thank you for agreeing to help us make a determination concerning the disclosure of personal information under section 17(2) of the *Freedom of Information and Protection of Privacy Act*. This section provides that the head of a public body may refuse to disclose to an applicant personal information about the applicant if, in the opinion of a physician, a chartered psychologist or a psychiatrist, or any other appropriate expert depending on the circumstances of the case, the disclosure could reasonably be expected to result in immediate and grave harm to the applicant's health or safety.

As we have already discussed with you, we wish you to provide an expert opinion as to whether or not [*specify general nature of records and health or safety issue*] could reasonably be expected to result in immediate and grave harm to [*name of applicant*]'s [*health or safety depending on the circumstances*]. However, before releasing the personal information to you, we need to explain to you and obtain your agreement to certain conditions regarding the use and handling of that information which are imposed by section 5 of the Freedom of Information and Protection of Privacy Regulation.

First, you must not use the information except for the purposes of determining whether or not disclosure of the records could reasonably be expected to result in immediate and grave harm to the individual's [*specify issue of health or safety*].

Second, you accept responsibility for maintaining the security and confidentiality of all personal information found in the records and of any notes you may create from the records.

Third, you agree to [*either return all the records and destroy all notes created from the records or destroy all copies of the records and notes taken from them*] after you have completed the determination and reported to us.

Model Letter U – Initial Letter to Expert under Section 17(2) (continued)

Once again we thank you for your cooperation. These conditions are established by the Regulation to protect the privacy of the individual involved and probably reflect confidentiality practices which you already observe in your daily professional activities.

Space is provided at the bottom of this letter for you to indicate, through your signature, that you accept these conditions. Please return the letter to us at [*name and address of public body*]. If you agree to help us in making this determination about disclosure of the information, the records will be forwarded to you shortly.

If you have any questions about the process or section 17(2), do not hesitate to contact me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

I agree to the conditions set out above.

____
[*Signature of expert*]

Model Letter V – Letter Transmitting Records to Expert under Section 17(2)

Purpose: *To transmit records to an expert for the determination as to whether or not to disclose personal information to an applicant under section 17(2) after they have agreed to the conditions of this process in Model Letter U.*

[*Reference number*]

[*Date*]

[*Name and address of expert*]

Dear [*Name of expert*]:

[*Name of public body*] has received your response to our letter of [*date of Model Letter U*].

Thank you for agreeing to assist us in making a determination whether or not to disclose personal information under section 17(2) of the *Freedom of Information and Protection of Privacy Act*, and for accepting the conditions placed on this assessment.

The records under consideration are enclosed. We would very much appreciate having your opinion by [*date*].

When you have completed your review, please return the records to [*name and address in public body*]

OR

When you have completed your review, please destroy the records in accordance with the agreement that we have in place with you.

If you have any questions about the process or section 17(2), do not hesitate to contact me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Attachment

Appendix 4

Privacy Reviews and Compliance Audits

Appendix 4
Privacy Reviews and Compliance Audits

Overview

Implementation of **Part 2** of the *FOIP Act* should be based on a review of existing systems used to collect, maintain, use and disclose personal information. Systems should be reviewed periodically to ensure ongoing compliance.

The Office of the Information and Privacy Commissioner conducts investigations in public bodies concerning compliance with **Part 2** of the *FOIP Act*. Such investigations may take the form of an audit. This can deal with either a public body generally or with a specific program that collects, and uses significant amounts of personal information. It will include a number of questions for the FOIP Coordinator and program managers, and in-depth interviews to determine practices and procedures. An investigation may be the result of a complaint received by the Commissioner, may be requested by the public body, or may be initiated by the Commissioner to ensure compliance.

This appendix provides some criteria and questions that may help in establishing an internal review process and in preparing for the type of investigation that the Commissioner may initiate.

The FOIP Coordinator should be able to respond in a reasonable and positive fashion to each of the following groupings of queries for each personal information system. The responses will determine whether or not there is general compliance with **Part 2** of the *Act* for each system and the program it supports. In this context, systems are both automated computer systems and manual processes.

Review Criteria and Questions

For each personal information system determine:

1. *Controls on Collection*

(a) What personal information is collected? This should be described by generic type, such as name, date of birth, income level, etc., or by data element.

(b) Does the public body have authority to collect the particular personal information in the system? Is the collection:

- authorized by or under an Act or Regulation of Alberta or Canada;
- collected for purposes of law enforcement; or

- related directly to and necessary for an operating program or activity?

If none of these criteria apply, then there is no authority for collecting the personal information.

(c) Are there collection control and approval mechanisms in place to ensure that the minimum amount of personal information necessary to carry out the program or activity is collected?

If the answer is no, consideration should be given to establishing such control and approval mechanisms.

The objective here is to:

- seek to clarify authorizations for the collection of personal information;
- eliminate any collection of personal information which does not meet the criteria set out in **section 32** of the *Act* and amend collection instruments, contracts and agreements, and policies and procedures which require the collection of this personal information accordingly; and
- implement administrative controls which continue to ensure that all new or modified collection of personal information meets the criteria set out in **section 32** and is based on the minimum amount of personal information necessary to meet program needs.

(d) Is the information collected directly from the individuals to whom it relates?

(e) If not, which exception to direct collection applies under **section 33(1)**?

If no exception applies or can be applied, then the information must be collected directly from the individual to whom it relates and operational practices will have to be changed. It may be possible to obtain consent from individuals for indirect collection when such collection benefits the individuals. An example would be when it saves completing a second application for a benefit or entitlement.

(f) Are there written policies and procedures governing the collection of personal information? Do these reflect the requirements of **Part 2** of the *FOIP Act*?

(g) What is the method of collection and is this designed to adequately inform the individual of the purpose of the collection of personal information? Methods include face-to-face interview, telephone interview, form or questionnaire, and direct electronic input.

Is there an ongoing process in place to ensure that collection instruments in all formats inform individuals about the purposes of collection?

(h) Does the public body or its agents collect and hold only that personal information necessary to deliver the program or service?

(i) Are procedures in place to permit the public body to periodically review its needs for personal information connected to the program or service? This should be done at least once every five years or more frequently if there are changes to the program of service.

2. Accuracy

Are there measures in place to ensure that personal information used to make decisions directly affecting individuals is accurate and complete? Describe these measures.

(a) Is there a record of when the file containing the personal information was last updated?

(b) Is there a record of the source of the information used to update the file?

3. Access and Correction

(a) Are there written procedures to accommodate access requests by individuals for information about themselves?

(b) What steps are taken to ensure the access request is from the individual to whom the information applies?

(c) What procedures govern the public body in correcting personal information if requested to do so by the individual, or annotating the information if a correction is not made?

(d) Is there a system in place to enable public bodies and third parties that have received personal information for which a correction is requested within one year of the request to be notified and requested to update their files?

(e) Are individuals adequately notified that a correction or annotation has been made?

(f) Are individuals being advised of their right, where applicable, to complain to the Information and Privacy Commissioner about a refusal to make a correction?

4. Protection

(a) Does the public body have a security policy and practices and procedures that meet the requirements of **section 36** of the *FOIP Act*?

(b) Are security responsibilities clearly defined? Describe these responsibilities and name the person(s) accountable for security.

(c) Has a security review that includes protection of personal information been undertaken recently and, if so, were any deficiencies identified? Describe deficiencies and measures to correct them.

(d) Are there problems with personal information being stored in insecure facilities or conditions, including facilities and conditions during transfer to and storage at a records centre?

(e) Is personal information, including electronic data, being disposed of under secure conditions? Describe practices and procedures.

5. Controls on Use

(a) For what purpose(s) is the information used?

(b) If any purpose is other than the purpose for which the information was collected or compiled, is the use:

- consistent with the original purpose;
- consented to by the individual in the prescribed manner;
- a purpose for which the information may be disclosed to the public body under **sections 38**, **40**, or **41** of the *Act*?

If none of these conditions applies, then the personal information is being used in contravention of **Part 2** of the *FOIP Act*.

6. Controls on Disclosure

(a) Is personal information being disclosed to other public bodies or third parties?

(b) If so, what is the authority for disclosure under **section 38(1)** of the *Act*?

If no provision under **section 38** authorizes a disclosure to take place, it is being done in contravention of **Part 2** of the *FOIP Act*.

(c) If your organization is a provincial government body, is a record of any consistent use or disclosure attached or linked to the record of personal information? Are procedures in place to ensure that such recording occurs?

(d) Is personal information shared with other levels of government, their agencies or other public bodies? Specify which governments, agencies or other public bodies.

(e) If so, is it authorized by an enactment of Alberta or Canada, an agreement or arrangement, consent, or is it for delivery of a common or integrated program? Provide a general description of the privacy provisions of the enactment, agreement, arrangement or common or integrated program.

(f) Who within the public body uses the information? Do people outside the public body use the information? What authority permits such disclosure and use, and what privacy protection provisions are in place governing the handling of the personal information?

(g) How are individuals informed of their right to request non-disclosure of personal information described in **section 16(2)(j)** of the *Act* so that the public body can comply with **section 16(3)**? What steps have been taken to ensure that the public body does not disclose such information when requested not to do so?

7. *Data Matching*

(a) Does data matching take place in regard to personal information in the system, either internally to your organization or externally?

(b) Is the data matching for a purpose that does not involve making a decision about an individual (see Chapter 9 of this publication)?

(c) If not, what is the authority under **Part 2** of the *Act* for the data matching?

(d) Are procedures and practices in place to ensure that all data matching activities are conducted in accordance with the data matching policy and guidelines?

(e) Is the Information and Privacy Commissioner notified of all data matching outside the established exclusions and given the opportunity to provide comments and recommendations?

8. *Consistent Uses*

(a) Do all consistent uses meet the definition in **section 39** of the *Act*?

If they do not, then it will be necessary to find another basis for the use or disclosure or cease the practice.

(b) Are new consistent uses recorded or linked to the information to which they apply? Is there a program to add these uses to the descriptions in the public body's directory of personal information banks?

9. Research or Statistical Purposes

(a) Is identifiable personal information disclosed for research or statistical purposes?

(b) If so, does the disclosure follow the requirements of the *Act* and FOIP Regulation and the guidance of the Model Research Agreement?

(c) Are there written procedures and practices in place to guide the process of deciding whether or not to disclose identifiable personal information for research or statistical purposes? Describe them.

10. Management of Personal Information

(a) Has a person been appointed to be accountable for each personal information bank or system?

(b) Have the needs for managing personal information been integrated into the record-keeping management principles and practices of the organization? If so, describe the general principles.

(c) Is any personal information in electronic form? If so, is this personal information managed in the same way as hard copy records? If not, describe the principles and practices applied to electronic records.

(d) Does the public body maintain duplicate copies of personal information in different systems? If so, how is the management of the different systems integrated to ensure that privacy protection requirements are met in the same way? Describe the procedures and practices used.

(e) Is a Privacy Impact Assessment conducted when designing and implementing new or modified programs or services requiring the collection and handling of personal information systems or in applying technology to personal information systems? If so, describe the approach, policy, procedures, practices and accountability framework that is in place.

11. Retention

(a) Does the public body have in place a records retention and disposition schedule for the personal information system which has been approved by the appropriate governing body, and does it dispose of personal information in accordance with the schedule?

(b) Is all personal information used to make decisions directly affecting an individual retained for at least one year after the decision is made? How is compliance monitored?

(c) Is personal information retained for purposes other than that for which it is collected? If so, explain the reasons for retention, the form of retention and controls over disposal. Any retention must meet the requirements of the *FOIP Act*.

(d) Are procedures in place for the disposal of personal information, including information in electronic form, which protects it from unauthorized disclosure until disposal is completed? Describe these procedures and the method of their application.

(e) Do these procedures take into account the disposal of equipment such as computers, diskettes and filing cabinets that may have personal information stored within them? What are these and how are they applied?

12. Contracting

(a) Is personal information collected, used or disclosed to contractors in carrying out programs or services or managed by them on behalf of the public body?

(b) If so, what provisions are in place to ensure that the contractor meets the privacy protection requirements of **Part 2** of the *FOIP Act*?

13. Policies and Procedures

(a) Have written policies and procedures relating to the protection of privacy been developed for the program or service? If so, list and describe these.

(b) How widely are these distributed?

(c) How are employees, including contractors, volunteers and appointees to boards or committees, made aware of these policies and procedures?

(d) Are the policies and procedures complete and do they accurately reflect the requirements of the *FOIP Act*?

Appendix 5

Model FOIP Request Charts

Appendix 5
Model FOIP Request Charts

Chart 1—Model FOIP Request (No Extension to Time Limit)

Key Tasks	Timelines - Calendar Days	Manual References	FOIP Tips
Request received by FOIP office. Decision: Routine access to information or FOIP request.	Day of Receipt	1.8 Accessing Information 1.9 Routine Access to Information 3.3 Receiving a FOIP Request/ Duty to Assist Applicants/ Clarifying Requests	Provide information through routine channels if possible.
Thirty Day Clock Starts	**30 calendar days to respond**		
If access request--initial fee paid? Is it a request for access to information or for the applicant's own personal information? Is it a continuing request? Clarify request with applicant. Decide whether request should be transferred. Send acknowledgement to applicant. Notify applicant if transferred.	**Day 1 - first working day after receipt** **Clock does not start until initial fee is paid**	1.6 Custody or Control 3.3 Receiving a FOIP Request/ Nature of Request/ Continuing Request/ Clarifying Requests/ Transferring a Request	Clarify what is wanted with applicant if not clear. Always be helpful and keep applicant informed. Do not probe motives. Send letter to applicant if initial fee was not received for a general access request. Check with other public body for consent before transfer.
Set up request file. Ask program areas to search for records. Log receipt of request on paper or electronic tracking system.	**Day 2**	3.3 Receiving a FOIP Request/ Documenting and Tracking Requests 3.4 Processing a FOIP Request/ Locating Records	Information about applicant is only shared on "need to know" basis. Ensure all potential program areas are asked to search for records. Search paper and electronic records.

Key Tasks	Timelines - Calendar Days	Manual References	FOIP Tips
Program areas retrieve records and forward originals to FOIP Coordinator. Consider need for time extension if extensive records to be searched. Copy retrieved records.	**Days 2 – 7**	3.3 Receiving a FOIP Request/ Response Time Limits 3.4 Processing a FOIP Request/ Locating Records	Search for all relevant records, including working and electronic files. Keep accurate and complete documentation of search. Make 3 copies of each record and number all documents.
Consider fees and send estimate if applicable with request for deposit. Consider need for consultations within public body and with other public bodies. Consider need for third party consultation. Consider creation of a record. If applicable, send notices to third party—see Chart Two for process.	**Days 7 – 10** **If fee estimate is sent to applicant, clock stops until deposit is received.**	3.4 Processing a FOIP Request/ Preliminary Assessment/ Assessing Fees/ Creating a New Record 5 Third Party Intervention and Notices	Have all relevant records been located? Use fee estimate form as a guide. Stop request processing until deposit is received. Consider fee waiver and/or narrowing request. Executive Council or Treasury Board must be consulted regarding cabinet confidences.
Internal consultations. External consultations. Consider whether time extension is needed to complete consultations. Preliminary assessment complete, consultations in process.	**End of Day 10**	3.3 Receiving a FOIP Request/ Response Time Limits	Consult with program areas for context and sensitivity. Consult externally, i.e. key government departments or local public bodies.

Key Tasks	Timelines - Calendar Days	Manual References	FOIP Tips
Detailed line-by-line review. Incorporate results of consultations into review—ongoing. Apply exceptions.	**Days 10 – 17**	3.4 Processing a FOIP Request/ Line-by-Line Review of Records/ Severing Information 4 Exceptions to the Right of Access	Continue consultation with program areas. Keep accurate and complete record of reasons for each exception. Keep accurate records of time spent serving records if fee estimate was issued.
Last day for transferring request.	**Day 15**	3.3 Receiving a FOIP Request/ Transferring a Request	Notify applicant.
FOIP Coordinator reviews recommendations and incorporates results of consultations. Consider whether time extension is needed to deal with outstanding external consultations.	**Day 17 – 21**	3.3 Receiving a FOIP Request/ Response Time Limits	Advise senior management and communications or significant issues. Encourage pubic bodies to respond immediately to avoid time extension.
Final consultations, internal and external completed.	**End of Day 23**		
Final analysis of review and recommendations. FOIP Coordinator makes final recommendations to decision maker or makes final decisions.	**End of Day 25**		Discuss any sensitive or major issue with Head or senior management.
Make any changes required by Head or final decision maker. Prepare records for delivery to applicant.	**Days 25 - 27**	3.4 Processing a FOIP Request/ Severing Information	

Key Tasks	Timelines - Calendar Days	Manual References	FOIP Tips
Finalize fee if necessary, and inform applicant in writing of balance owing.	**Day 27** **Clock stops until balance of fee received**	3.4 Processing a FOIP Request/ Deposits and Payment of Fees	
Final response letter to applicant, enclosing records or stating how they may be obtained or examined. Close file.	**Day 30, or next working day if Day 30 falls on weekend or holiday.**	3.5 Responding to a FOIP Request.	Ensure all correspondence and documentation is on file.

Chart 2 - Model FOIP Request (Time Extended for Third Party Notice)

Key Tasks	Timelines - Calendar Days	Manual References	FOIP Tips
Request received by FOIP office. Decision: Routine access to information or FOIP request.	Day of Receipt	1.8 Accessing Information 1.9 Routine Access to Information 3.3 Receiving a FOIP Request/ Duty to Assist Applicants/ Clarifying Requests	Provide information through routine channels if possible.
Thirty Day Clock Starts	**30 calendar days to respond**		
If access request--initial fee paid? Is it a request for access to information or for the applicant's own personal information? Is it a continuing request? Clarify request with applicant. Decide whether request should be transferred. Send acknowledgement to applicant. Notify applicant if transferred.	**Day 1 - first working day after receipt** **Clock does not start until initial fee is paid**	1.6 Custody or Control 3.3 Receiving a FOIP Request/ Nature of Request/ Continuing Request/ Clarifying Requests/ Transferring a Request	Clarify what is wanted with applicant if not clear. Always be helpful and keep applicant informed. Do not probe motives. Send letter to applicant if initial fee was not received for a general access request. Check with other public body for consent before transfer.

Key Tasks	Timelines - Calendar Days	Manual References	FOIP Tips
Set up request file. Ask program areas to search for records. Log receipt of request on paper or electronic tracking system.	**Day 2**	3.3 Receiving a FOIP Request/ Documenting and Tracking Requests 3.4 Processing a FOIP Request/ Locating Records	Information about applicant is only shared on "need to know" basis. Ensure all potential program areas are asked to search for records. Search paper and electronic records.
Program areas retrieve records and forward originals to FOIP Coordinator. Copy retrieved records.	**Days 2 – 7**	3.5 Receiving a FOIP Request/ Response Timetable 3.3 Processing a FOIP Request/ Locating Records	Search for all relevant records, including working and electronic files. Keep accurate and complete documentation of search. Make 3 copies of each record and number all documents.
Consider fees and send estimate if applicable with request for deposit. Consider need for consultations within public body and with other public bodies. Consider need for third party consultation. Send notices to third party and applicant. Consider creation of a record.	**Days 7 – 10** **If fee estimate is sent to applicant, clock stops until deposit is received.**	3.4 Processing a FOIP Request/ Preliminary Assessment/ Assessing Fees/ Creating a New Record 5 Third Party Intervention and Notice	Have all relevant records been located? Use fee estimate form as a guide. Stop request processing until deposit is received. Consider fee waiver and/or narrowing request. Send third party notices as early as possible. Notify applicant of third party consultations and date by which release decision will be made. Executive Council or Treasury Board must be consulted regarding Cabinet confidences.

Key Tasks	Timelines - Calendar Days	Manual References	FOIP Tips
Decision on release of third party records made after response received from third party or 21 days after notice was given.			
Internal consultations. External consultations. Consider whether time extension is needed to complete consultations. Preliminary assessment complete, consultations in prccess.	**End of Day 10**	3.3 Receive a FOIP Request/ Response Time Limits	Consult with program areas for context and sensitivity. Consult externally, i.e. key government departments or local public bodies.
Detailed line-by-line review. Incorporate results of consultations into review—ongoing. Apply exceptions.	**Days 10 – 17**	3.4 Processing a FOIP Request/ Line-by-Line review of records/ Severing Information 4 Exceptions to the Right of Access	Continue consultation with program areas. Keep accurate and complete record of reasons for each exception. Keep accurate records of time spent serving records if fee estimate was issued.
Last day for transferring request.	**Day 15**	3.3 Receiving a FOIP Request/ Transferring a Request	Notify applicant.
FOIP Coordinator reviews recommendations and incorporates results of consultations Consider whether time extension is needed to deal with outstanding external consultants.	**Day 28-31**	3.3 Receiving a FOIP Request/ Response Time Limits	Advise senior management and communications or significant issues. Encourage pubic bodies to respond immediately to avoid time extension.

Key Tasks	Timelines - Calendar Days	Manual References	FOIP Tips
Consider response from third party. Make decision on release of record/severing and send letter to third party and applicant.	**Day 32-41**	5.6 Response from Third Party 5.7 Notice of Decision	Processing of records not subject to third party notice can continue.
Public body has 10 days to make decision on release of third party records. Once the decision is made, third party had 20 days to ask for review.			
Final consultations, internal and external completed.	**Days 42-57**		
Final analysis of review and recommendations. FOIP Coordinator makes final recommendations to decision maker or makes final decisions.	**End of Day 57**		Discuss any sensitive or major issue with Head or senior management.
Make any changes required by Head or final decision maker. Prepare records for delivery to applicant.	**Days 57-59**	3.4 Processing a FOIP Request/ Severing Information	
Finalize fee if necessary, and inform applicant in writing of balance owing.	**Day 59** **Clock stops until balance of fee received**	3.4 Processing a FOIP Request/ Deposits and Payment of Fees	
Final response letter to applicant, enclosing records or stating how they may be obtained or examined. Close file.	**Day 61, or next working day if Day 61 falls on weekend or holiday.**	3.5 Responding to a FOIP Request.	Ensure all correspondence and documentation is on file.

Appendix 6

Freedom of Information and Protection of Privacy Act Forms

Appendix 6
Freedom of Information and Protection of Privacy Act Forms

Request to Access Information form

Request Summary form

Transmittal Memorandum (sample)

Access Request Review form

Access Request Review Recommendation/Summary form

Access Request Review Attachment: Detailed Review of Records form

Request to Correct Personal Information form

Personal Information Annotation form

Law Enforcement Disclosure form

Authorization of Representative form

Affidavit for Witness form

Proposal to Access Personal Information for Research or Statistical Purposes form

Agreement for Access to Personal Information for Research or Statistical Purposes form

Office of the Information and Privacy Commissioner - Request for Review form

FREEDOM OF INFORMATION
AND PROTECTION OF PRIVACY

Request to Access Information

Personal information on this form is collected under Alberta's *Freedom of Information and Protection of Privacy Act* and will be used to respond to your request. Instructions for completing this form are on the back.

About you

☐ Mr. ☐ Ms ☐ Dr. ☐ Mrs. ☐ Miss	Last name		First name
Name of company or organization *(if applicable)*			
Mailing address			
City or town		Province	Postal code
Telephone (daytime) ( )	Telephone (evening) ( )	Fax number ( )	E-mail address

About your request

1. What kind of information are you requesting access to?
   - ☐ **General information** *(Please attach the initial fee of $25.)*
   - ☐ **Personal information** *(No initial fee is required for personal information.)*
2. To which public body are you making your request? *(Please fill in the name of the organization.)*
3. Do you want to: (a) receive a copy of the record? ☐ **OR** (b) examine the record? ☐

About the information you want to access

1. What records do you want to access? Please give as much detail as possible. *(If you want access to your personal information, be sure to give all your previous names. For another person's information, you must attach proof that you can legally act for that person. If you need more space, please attach a separate sheet of paper.)*
2. What is the time period of the records? Please give specific dates. *(See reverse for details.)*

Your signature

Signature	Date

For FOIP office use only:

Date received	Request number

How to complete the form

You can access many public body records without making a request under the *FOIP Act*. To determine whether you need to make a request under the *Act* or if you need help completing the form, contact the FOIP Coordinator of the organization to whom you are making the request.

About you

Check the title by which you prefer to be addressed and enter your last name and first name. Then enter the name of the company or organization that you are representing, if applicable. Enter your complete mailing address and your daytime and evening telephone numbers. The public body may need to contact you if they have any questions about your request. If you have a fax number or E-mail address where correspondence can be sent, enter them in the spaces provided.

About your request

If you need help to find out what records an organization has, please contact their FOIP Coordinator.

1. What kind of information are you requesting? Indicate whether you are requesting general or personal information.

   General information: If you are making a request for general information, there will be an initial fee of $25. You will be provided with an estimate of how much your request will cost before processing begins. If the total cost of processing your request is more than $150, you are asked to pay a 50% deposit. The records are provided when the fee is paid in full.

   Personal information: If you are requesting records containing your personal information, you will have to provide proof of your identity before the records are released to you. If you are requesting records for another person, you will have to provide proof that you have the authority to act for that person. For example, you might provide proof that you are the person's guardian or trustee or that you have power of attorney for the person. There is no fee for accessing personal information unless the cost of producing copies is more than $10. In these cases, you will be notified of the fee.

   If you are making a continuing request (the same request processed repeatedly at pre-determined time intervals over a period of up to 2 years), you should contact the FOIP Coordinator of the appropriate public body. The initial fee is $50 and you must pay any additional costs as the information becomes available.

2. Enter the name of the public body that you believe has the records that you want to access.
3. Do you want to receive a copy of the record or examine the record? Check the appropriate box.

About the information you want to access

1. What information are you requesting? Please be as specific as possible in describing the records. The more specific your request, the quicker and more accurately it can be answered. If you need more space, please continue your description on a separate sheet of paper and attach it to this request form.

   If you are requesting your own personal information, please be sure that you give:
   - your full name;
   - any other names that you have previously used; and
   - any identifying number that relates to the records, such as your employee number, case number or other identification number.

   If you are requesting another person's information, please give:
   - the person's full name;
   - any other name that person may have used on the records; and
   - any identifying numbers for the person if you know them.

   If you are requesting records for another person, you will have to provide proof that you have the authority to act for that person.

2. Enter the time period of the requested records. For example, if you are requesting records for the period January 1, 1993 to August 31, 1994, enter those dates in the space provided. If you want records from August, 1996 to present, enter "August, 1996 to present."

Your signature

Sign and date the form and send it to the FOIP Coordinator of the appropriate organization. If you are not sure of where to send the form, please consult the FOIP Coordinator of the organization that has the records you wish to access.

REQUEST SUMMARY
FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

Public Body Name

Region

Reporting Period

From **To**

REQUEST PROCESSING						EXCEPTIONS TO ACCESS OR PRIVACY CITED***																		
Request Number	Date Received	Date Closed	Source	Days*	Disposition**	11(2)	15(1)	15(2)	16	17	18	19	20	21	22	23(1)(a)	23(1)(b)	23(1)(c)	23(1)(d)	23(1)(e)	23(1)(f)	23(1)(g)	23(1)(h)	24
Total this page																								

* Number of Days to Complete the Request
** Disposition Code (from list at right)
*** Record all exceptions or exclusions, cited on the request (continued on page 2)

SOURCE OF REQUEST

A	Academic/Researcher
B	Business/Commercial
E	Elected Official
M	Media
P	General Public
O	Organization/Interest Group

ACCESS DISPOSITION CODES

A	Disclosed Completely
B	Disclosed Partially
C	Nothing Disclosed
D	Abandoned
E	Records Do Not Exist
F	Withdrawn
G	Transferred

Correction of Personal Information

H	Correction Made
I	Request Noted on Record
J	Notation Placed on Record
K	Other Disposition

REQUEST SUMMARY (Page 2)
FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

Public Body Name

Region

Reporting Period

From **To**

Continued			EXCEPTIONS CITED				EXCLUSIONS CITED																								
Request Number	Extension*	Release**	25	26	27	28	3(a)	3(b)	4(1)(a)	4(1)(b)	4(1)(b.1)	4(1)(c)	4(1)(c.1)	4(1)(c.2)	4(1)(d)	4(1)(e)	4(1)(e.1)	4(1)(f)	4(1)(g)	4(1)(h)	4(1)(i)	4(1)(i.1)	4(1)(j)	4(1)(k)	4(1)(l)	4(1)(m)	4(1)(n)	4(1)(o)	5
Total this page																														

* Extension - Reason and number of days required
ECO - Extension - Consultation with other public body
EBC - Extension by Commissioner under s. 13(1)
ECR - Extension - Clarify Request
EMC - Extension - Multiply Concurrent Requests
ESV - Extension - Search/Volume
ENT - Extension - Third Party Notice

** Release Status
C - Copies given
E - Examination
B - Both copies and examination
N/A - Not applicable

Transmittal Memorandum (sample)
(on public body memorandum paper)

Date:

To: [*Program Director*]

From: [*FOIP Coordinator*]

Re: [subject]

A request under the *Freedom of Information and Protection of Privacy Act* for records relating to [*subject*] was received on [*date*]. We have 30 calendar days until [*date*] in which to respond to it. I would appreciate your immediate attention in locating all relevant records pertinent to the request and a preliminary assessment undertaken in cooperation with my staff by [*date*]. The FOIP officer assigned to this case is [*name and telephone number*].

Attached is an Access Request Review form, an Access Request Review Recommendation/Summary form and a Detailed Review of Records form, which will assist you in documenting the activities and actions connected with the request. This record will be extremely important in developing the [*public body's*] case if the applicant makes a complaint to the Information and Privacy Commissioner.

You should be aware that it is an offence under the *Act* to alter, falsify or conceal any record or direct another person to do so (section 86(1)(c.1)), or to destroy any record (section 86(1)(e)) in order to evade a FOIP request for access to records. The penalty for an offence under section 86 is a fine of up to $10,000.

Please provide the name(s) of the member(s) of your staff assigned to deal with this request by [*date*] so that arrangements may be made for a meeting to discuss the [*public body's*] response.

If you have any questions, please call me at [*telephone number*].

[*FOIP Coordinator*]

Attachment

FREEDOM OF INFORMATION AND
PROTECTION OF PRIVACY

ACCESS REQUEST REVIEW

Request Type: ☐ General Information ☐ Personal Information

Name of Program or Branch:

Request No.:

PART 1 - GENERAL

METHOD OF ACCESS REQUESTED

☐ Examine Originals ☐ Copies (selected documents) ☐ Copies (all) ☐ Other (specify):________________________

TRACKING DATES

Date Received	Request Due Date	Revised Due Date	Request Closed Date

PROGRAM AREA(S) ASSIGNED TO PROCESS REQUEST

SUMMARY OF STAFF TIME SPENT ON REQUEST

Locate Records	Review Records	Sever Records	Prepare Response Pkg	Name(s)	Total Hours Spent
☐	☐	☐	☐	____________________	________
☐	☐	☐	☐	____________________	________
☐	☐	☐	☐	____________________	________
☐	☐	☐	☐	____________________	________

SUMMARY OF FREEDOM OF INFORMATION AND PRIVACY UNIT RECOMMENDATIONS

(Attach a separate sheet if the space below is not sufficient.)

Prepared by:
(type name and sign)

Approved by:
(type name and sign)

Freedom of Information and Privacy Coordinator

Title:

Date:

ACCESS REQUEST REVIEW - PAGE 2

Request No.:

PART 2: PROGRAM AREA RETRIEVAL AND REVIEW OF RECORDS

Program Area:	Program Area Contact:	Telephone No.:

LOCATION AND RETRIEVAL OF RECORDS

Search Done By: (name in print)	Start Date:	Target Completion Date:	Actual Completion Date:

Areas Searched (attach file lists, indices or other aids used in search):

Records Retrieved (by title - use attachment if necessary):

PROGRAM AREA REVIEW OF RECORDS

Records Reviewed By: (name in print)	Start Date:	Target Completion Date:	Actual Completion Date:

SUMMARY OF PROGRAM AREA RECOMMENDATIONS

Approved By (program director): (type name and sign)

Date:

ACCESS REQUEST REVIEW RECOMMENDATION / SUMMARY

FREEDOM OF INFORMATION
AND PROTECTION OF PRIVACY

Request Type: ☐ General Information ☐ Personal Information

Name of Program or Branch:

Request No.:

To:

Date:

From:

Name of Applicant:

Records / Information Requested:

Number of Files / Pages Reviewed:

Types of Information Contained in the Records:

Exceptions Recommended:

Application of Discretionary Exceptions (summarize reasons):

Application of Mandatory Exceptions (summarize reasons):

Severing Required (summarize reasons):

Prepared by:
(signature)

Approved by:
(signature)

Title:

Date:

Title:

Date:

FREEDOM OF INFORMATION
AND PROTECTION OF PRIVACY

ACCESS REQUEST REVIEW ATTACHMENT: DETAILED REVIEW OF RECORDS

(use multiple sheets if necessary)

Request No.:	**Name of Public Body:**	**Program Area:**	**Program Area Contact:**	**Telephone No.:**

Document No.	No. of Pages	Document Date	Document Description	Exceptions Applied	Comments / Explanations	Third Party Notice or Consultation (Yes or No)

FREEDOM OF INFORMATION
AND PROTECTION OF PRIVACY

Request to Correct Personal Information

Personal information on this form is collected under Alberta's *Freedom of Information and Protection of Privacy Act* and will be used to respond to your request. Instructions for completing this form are on the back.

About you

☐ Mr. ☐ Ms ☐ Dr. ☐ Mrs. ☐ Miss	Last name		First name
Name of company or organization *(if applicable)*			
Mailing address			
City or town		Province	Postal code
Telephone (daytime) ( )	Telephone (evening) ( )	Fax number ( )	E-mail address

About your request

1. Whose information do you want to correct?

☐ Your own personal information
☐ Another person's information *(Please attach proof that you can legally act for the person.)*

2. To which public body are you making your request? *(Please fill in the name of the organization.)*

About the information you want to correct

1. What personal information needs to be corrected? Please give as much detail as possible. *(Be sure to give the complete name that is in the records if it is different from the name given above. If you need more space, please attach a separate sheet of paper.)*

2. What correction do you want to make and why? *(Please attach any documents that support your request.)*

Your signature

Signature	Date

For FOIP office use only:

Date received	Request number

IMPB/JUNE 1998

How to complete the form

You can correct information in many public body records without making a request under the *FOIP Act*. To determine whether you need to make a request under the *Act* or if you need help completing the form, contact the FOIP Coordinator of the organization to whom you are making the request.

About you

Check the title by which you prefer to be addressed and enter your last name and first name. Then enter the name of the company or organization that you are representing, if applicable. Enter your complete mailing address and your daytime and evening telephone numbers. The public body may need to contact you if they have any questions about your request. If you have a fax number or E-mail address where correspondence can be sent, enter them in the spaces provided.

About your request

1. Whose information do you want to correct? Indicate whether you want your personal information or another person's information to be corrected.

   Your personal information: If you want your records to be corrected, you will have to provide proof of your identity.

   Another person's information: If you want the records of another person to be corrected, you will have to provide proof that you have the authority to act for that person. For example, you might provide proof that you are the person's guardian or trustee or that you have power of attorney for the person.

2. Enter the name of the public body that you believe has the records that you want to correct.

About the information you want to correct

1. What records contain the information that you want corrected? Please be as specific as possible in describing the records. The more specific your request, the quicker and more accurately it can be answered. If you need more space, please continue your description on a separate sheet of paper and attach it to this request form.

   If you want a correction made to your own personal information, please be sure that you give:
   - your full name;
   - any other names that you have used on the records; and
   - any identifying number that relates to the records, such as your employee number, case number or other identification number.

   If you want a correction made to another person's information, please give:
   - the person's full name;
   - any other name that person may have used on the records; and
   - any identifying numbers for the person if you know them.

2. What corrections do you want made? What is incorrect about the information that is currently on the record? Please be specific.

Your signature

Sign and date the application and send it to the FOIP Coordinator of the appropriate organization. If you are not sure of where to send the form, please consult the FOIP Coordinator of the organization that has the records you wish to correct.

Personal Information Annotation

FREEDOM OF INFORMATION
AND PROTECTION OF PRIVACY

Name of personal information bank:	**Number of personal information bank:**	**Reference number:**

In response to our refusal to make a correction to the record of ______________________________
(name of individual)

correction request date ______________________________ , we are making the following annotation
(date)

to the record, file or database.

This notation has been sent to the individual and to all public bodies and organizations to which the information was disclosed in the year preceding the registration date of the Request for Correction of Personal Information.

Authorized official or employee (type name and sign):	**Date:**

Law Enforcement Disclosure
Request for Disclosure under Section 38(1)(o) of the Freedom of Information and Protection of Privacy Act

FREEDOM OF INFORMATION
AND PROTECTION OF PRIVACY

Date:

In accordance with section 38(1)(o) of the *Freedom of Information and Protection of Privacy Act*, the

________________________________ hereby requests disclosure of personal
(name of public body)

information pertaining to ________________________________, which may be
(name of individual or other identifier)
generally described as:

____ .
(general description of information requested)

This information is required by this public body to assist in an investigation pursuant to:

____
(reference to a federal or provincial statute by section or description of purpose)

Name of requesting official	Title of requesting official
Signature of requesting official	Badge number (if applicable)

I, hereby ☐ consent to or ☐ refuse
this disclosure of personal information to

____
(name of public body)

Any personal information disclosed forms part of personal information bank(s)

____
(identify personal information banks if authorizing disclosure)

Name of authorized official	Title of authorized official
Signature of authorized official	Name of public body

NOTE: THIS COMPLETED DOCUMENT MAY QUALIFY FOR EXCEPTION TO DISCLOSURE UNDER SECTION 19 OF THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Authorization of Representative

FREEDOM OF INFORMATION
AND PROTECTION OF PRIVACY

I, ______________________________, living at ______________________________,

______________________________, in the province of ______________________________,

designate ____

living at ______________________________, ______________________________,

in the province of ______________________, as my personal representative to act on my behalf,

and to exercise (check one of the following):

☐ all my rights under the *Freedom of Information and Protection of Privacy Act*

☐ my right to access all my records containing personal information in all categories of personal information

☐ my right to access all records containing personal information or all categories of personal information following (number and titles of records or categories):

____

____

☐ The rights that are conferred on me under the *Freedom of Information and Protection of Privacy Act* in regard to the following questions:

____

____

I ratify and confirm by all present that my representative is conferred with all the responsibilities of the acts and the execution of said responsibilities on my behalf.

The present authorization will be in effect until ______________________, 20____.

SIGNED BY ______________________________ in the presence of:

____
Witness

Affidavit for Witness

Canada
in the Province of Alberta

I ____________________, __________________ of ____________________________
(name of the witness in full) (occupation of witness) (complete home address of witness)

in the province of _____________________________________, make oath and say that:

1. I was personally present and I saw _______________________________ sign the
(name of person)
Authorization of Representative to which this is attached.

2. The Authorization of Representative was signed by ________________________
(name of the person)
at __________________________________in the province of

________________________ and that I am the one who witnessed the document.

3. I know _________________ and I believe that he/she is 18 years of age or older.
(name of person)

____
Signature of Witness

Sworn before me at __________________________

in the province of ___________________________

on _______________________________________

____
Commissioner for Oaths

____
(print name here)

My Commission expires _______________, 20___

[*NAME OF PUBLIC BODY*]

PROPOSAL TO ACCESS PERSONAL INFORMATION FOR RESEARCH OR STATISTICAL PURPOSES

This form is used to request access, for research or statistical purposes, to personal information contained in records covered by the *Freedom of Information and Protection of Privacy Act* (the *Act*). If this request is approved by [*name of public body*], you will be asked, prior to being provided access to records containing personal information, to sign a legal agreement that ensures that individuals' privacy will be protected when the information is in your custody.

The collection of the information on this form is authorized by the *Act* and will be used only to evaluate and administer the request for access to personal information for the purpose of research. [*Name of contact, title, name of public body, business address and telephone number*] can answer any questions concerning this proposal or the collection of the information on this form.

Completeness and clarity will assist the [*name of the public body*] to assess this proposal quickly.

Note: A fee may be charged to provide this information. An estimate of the fee will be provided in advance.

Identification of Researcher

____
Name (last name/first name/initials)

Address: ______________________________ Telephone: ____________________
______________________________ Fax: ____________________
______________________________ E-mail: ____________________

Please provide the following additional information if applicable:

Institutional, Society or Corporate Affiliation: ______________________________
(include department if relevant)

Position: ______________________________

Academic Advisor (if student): ______________________________

Please also provide a curriculum vitae including the following information: education, research experience, and knowledge of subject.

Description of Research Project

Please attach the following information:

1) A general description of the research project (include the objectives of the project and the proposed method(s) of analysis).
2) An explanation of why the research project cannot be accomplished without access to personal information in individually identifiable form (i.e., personal information about named or identifiable individuals).
3) A detailed explanation of how the personal information will be used, including a description of any proposed linkages to be made between personal information in the records requested and any other personal information.
4) The expected period of time during which access to these records may be required.
5) The expected period of time during which these records will be used.
6) The benefits to be derived from the research project.
7) You must protect the security and confidentiality of the personal information that will be in your custody and ensure that unauthorized disclosure does not occur. What security measures do you propose to put in place?

Has funding to complete the project already been approved or received?

Yes ___ No ___

If funding is not already in place, explain the conditions and circumstances that will allow the project to be completed.

____

____

____

Please add any other information that you believe will assist [*name of public body*] in assessing this application.

____

____

____

____

____

____

Records Requested (Use additional sheets as required)

Please describe all records containing personal information to which access is requested. Provide as much detail as possible. Access will be given only to records listed below and only for the purposes approved for the research project description above. Any changes or additions to this list after the application is submitted should be made in writing and will require approval in writing from [*name of public body*].

____

____

____

____

____

Originals may be viewed only at [*name of public body*]. Will you require that the above records be copied (at your expense) for viewing elsewhere?

Yes ____ No ___

For Public Body Use Only

The application for records pursuant to Section 40 or Section 41 of the *Act* is approved subject to terms and conditions of a corresponding research agreement.

____
Signature

____
Position

____
Date

[*NAME OF PUBLIC BODY*]

AGREEMENT FOR ACCESS TO PERSONAL INFORMATION FOR RESEARCH OR STATISTICAL PURPOSES

This agreement is used once a proposal to access personal information for research or statistical purposes has been approved. Once the researcher has signed this form and the terms and conditions of access have been approved by the [*name of public body*], it becomes a legal agreement between the researcher and [*name of public body*]. The application must be appended to this agreement and forms part of the legal agreement.

The collection of the information on this form, is authorized by the *Act* and will be used only to administer the research project. [*Name of contact, title, name of public body, business address and telephone number*] can answer any questions concerning this agreement or the collection of the information on this form.

Identification of Researcher

____
Name (last name/first name/initials)

Address: ______________________________ Telephone: ____________________
______________________________ Fax: ____________________
______________________________ E-mail: ____________________

Please provide the following additional information if applicable:

Institutional, Society or Corporate Affiliation: ______________________________
(include department if relevant)

Position: ______________________________

Academic Advisor (if student): ______________________________

Description of Research Project

The research project for which the accessed records will be used is hereafter referred to as ____________________

____

____

Details of the purpose of the research, how the information will be used, and linkages that will be done are included in the Proposal for Access to Personal Information for Research or Statistical Purposes which is appended to this agreement and is part of this legal agreement.

Records Requested (Use additional sheets as required)

Only those records requested in the Proposal for Access to Personal Information for Research or Statistical Purposes, appended to this application will be provided ("these records"). Any changes or additions to the list must be made in writing and will require approval in writing from [*name of public body*]. Clarification of the records to be accessed is shown below if required.

____

____

____

____

____

In the event that there is a difference between the records requested above and the records requested in the Proposal to Access Personal Information for Research or Statistical Purposes, the information in this agreement governs the agreement.

Fee

I understand that I am responsible for paying any fees incurred to search for, copy and or provide the requested records.

The estimated fee is ________________________.

I understand that this estimate may be revised at any time by [*name of public body*] and any revision will be made in writing.

Terms and Conditions of Access

I understand and will abide by the following terms and conditions:

Security

1) I understand that I am responsible for maintaining the security and confidentiality of all personal information found in or taken from these records.

2) Apart from myself, **only** the following persons will have access to this personal information in a form that identifies or could be used to identify the individual(s) to whom it relates:

____
____
____

Before any personal information is disclosed to these persons, I will obtain a written agreement from each of them to ensure that they will not disclose that information to any other person and that they will be bound by all terms and conditions of the present agreement. I will keep a copy of each such agreement, and will provide [*name of public body*] with a photocopy.

3) None of these records (including copies of them or notes containing personal information taken from them) will be left unattended at any time, except under the conditions described in Paragraphs 4,5 and 6, below. If I am using these records on the premises of [*name of public body*], I will comply with [*name of public body*]'s security procedures.

4) Any copies of the requested records and any notes which contain personal information taken from them will be kept at the following address(es):

____________________ ____________________
____________________ ____________________
____________________ ____________________
____________________ ____________________

No records will be removed from the above premises without the prior written consent of [*name of public body*].

5) Physical security at the above premises will be maintained by ensuring that the premises are securely locked, except when one or more of the individuals named in Paragraph 1 are present, as well as by the following additional measures (e.g., locked filing cabinet):

____
____

6) **Individually identifiable information from the requested records will be maintained on a computer system to which users other than those listed in Paragraph 1 have access.**

Yes ___ No ___

If yes, access to the information will be restricted through the use of passwords and by other computer security measures that prevent unauthorized access, and trace such unauthorized access, including the following methods:

____

____

7) [*Name of public body*] will be permitted to carry out on-site visits and such other inspections or investigations that it deems necessary to ensure compliance with the conditions of this agreement.

Use of Personal Information

8) Personal information contained in the records which are requested in this application will not be used or disclosed for any purpose other than the research project described in this application (including additional linkages between sources of personal information), nor for any subsequent purpose, without the express written permission of [*name of public body*].

9) Papers or any other works which describe the results of the research undertaken will be written and/or presented in such a way that no individuals in the requested records can be identified and no linkages can be made between any personal information found in the requested records and personal information that is publicly available from other sources. There will be no exceptions to this rule without prior and specific written permission from [*name of public body*].

10) Any case file numbers or other individual identifiers to be recorded on computer will be created by myself or one of the persons listed in Paragraph 1 and will not relate to any real case numbers found in the records. Any such identifiers are to be used for statistical purposes only.

11) No case file numbers or other individual identifiers assigned for the purposes of the research project will appear in any other work.

12) No personal information that identifies or could be used to identify the individual(s) to whom it relates will be transmitted by means of any telecommunications device, including telephone, fax, modem, and cable.

13) Unless expressly authorized in writing by [*name of public body*], no direct or indirect contact will be made with the individuals to whom the personal information relates.

14) Individual identifiers associated with the records described in this application and agreement, or contained in copies of them, will be removed or destroyed at the earliest time at which removal or destruction can be accomplished consistent with the research purpose. At the latest, this will occur by:

______/______/______
(year/month/day)

Any extension to this time limit must be approved in writing by [*name of public body*]. The removal of individual identifers will be done in a manner that ensures that remaining personal information (including any found in research notes) cannot be used to identify the individual to whom it relates. **If necessary, this will be done by destroying copies of requested records or pages of notes in their entirety.** All destruction or removal of individual identifiers will be confidential and complete in order to prevent access by any unauthorized persons.

15) I understand that I am responsible for ensuring complete compliance with these terms and conditions. In the event that I become aware of a breach of any of the conditions of this agreement, I will immediately notify [*name of public body*] in writing.

16) I understand that the *Freedom of Information and Protection of Privacy Act* specifies that a person who under the *Act* wilfully violates the *Act*'s requirements for collection, use and disclosure of personal information is guilty of an offence and liable to a fine of up to $10,000. In addition to liability for an offence, I understand [*name of public body*] may take legal action against me if there is contravention of the terms and conditions of this agreement.

17) Written consent of [*name of public body*] must be obtained prior to the transfer of this agreement to another person, or a change in the use of the information is implemented. Consent may be arbitrarily withheld in the sole discretion of [*name of public body*].

18) [*Name of public body*] will receive a copy of the final research product.

Signed at ________________________________, this ______ day of __________________, 20_____.

____
Signature of Researcher

____
Signature of Witness

____
Name and Position of Witness

For Public Body Use Only

The terms and conditions of this agreement are hereby approved. [*Name of public body*] reserves the right to withdraw access to records without prior notice if this becomes necessary under the *Act*.

The expiry date for access to the records listed in this application and agreement is: ______/______/______ (year/month/day)

____
Signature

____
Position

____
Date

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

REQUEST FOR REVIEW

To: **Information and Privacy Commisioner**
Suite 410, 9925-109 Street
Edmonton, Alberta T5K 2J8

My Name Is:

My Mailing Address Is:

A telephone number where I can
be reached during the day is:

On ______________ I applied for information from the following source:
Date

OR:

On ______________ I asked to have my information corrected by the following source:
Date

OR:

On ______________ I was told by that information about me is going to be disclosed by the following source:
Date

OR:

I am concerned about the following:

AND:

I am requesting a review by the Commissioner because:

(It would be helpful if you attach a copy of any correspondence you have received from the source you referred to.)

Signature

Date

If you have any questions, please call (780) 422-6860

This office will forward a copy of your completed form to the head of the public body concerned and to any other person who in the opinion of the Commissioner is affected by the request. If concerns arise regarding this procedure, please make them known to the Commissioner as soon as possible.

Date Stamp Information and Privacy Commissioner

Index of

Freedom of Information and Protection of Privacy Act and Regulation Citations

Freedom of Information and Protection of Privacy Act and Regulation Citations

Freedom of Information and Protection of Privacy Act

Part 1 188
section 1(1)(d) 2
section 1(1)(e) 84
section 1(1)(f)(i) 23
section 1(1)(f)(i.1) 23
section 1(1)(f)(ii) 23
section 1(1)(f)(iii) 23
section 1(1)(g) 2
section 1(1)(h) 105, 211
section 1(1)(i) 2
section 1(1)(j) 2
section 1(1)(n) 6, 82
section 1(1)(p) 1, 3
section 1(1)(q) 5
section 1(1)(r) 74, 167
section 1(1)(s) 73, 147
section 2 1
section 2(a) 67
section 2(c) 67
section 3(a) 4, 15, 165
section 3(b) 4, 242
section 3(c) 4
section 3(d) 5
section 3(e) 5, 65, 210, 243
section 3(e)(ii) 249
section 4 7
section 4(1) 5, 292
section 4(1)(a) 7
section 4(1)(b) 7
section 4(1)(b.1) 8
section 4(1)(c) 8
section 4(1)(c.1) 9
section 4(1)(c.2) 9
section 4(1)(d) 9
section 4(1)(e) 9
section 4(1)(f) 10
section 4(1)(g) 10
section 4(1)(h) 10
section 4(1)(i) 11, 12
section 4(1)(i.1) 12
section 4(1)(j) 12
section 4(1)(k) 12
section 4(1)(l) 12, 124
section 4(1)(m) 13
section 4(1)(n) 13
section 4(1)(o) 13
section 4(1.1) 12, 131
section 4(2) 7
section 4(3) 13
section 5 .... 24, 67, 68
section 5(2) 14, 72, 242
section 6(1) 31, 60, 188
section 6(2) 57
section 6(3) 54
section 7(1) 33
section 7(2) 33
section 7(3) 33, 64
section 7.1 57
section 8 35
section 9 .... 8, 18, 51, 59, 288, 296, 301
section 9(1) 18, 34
section 9(2) 59
section 10 174
section 10(1) 41, 172
section 10(2) 42
section 11(1) 62, 96, 166
section 11(2) 65, 96
section 11(2)(a) 99, 117
section 11(2)(b) 95
section 12(2) 64
section 13 .... 38, 41, 42, 43, 44, 45, 54, 172, 174, 175, 288, 296, 301

section 13(1) 43, 44
section 13(1)(a) 38, 207
section 13(1)(b) 174, 207
section 13(1)(d) 42
section 13(2) 44
section 13(3) 43
section 13(4) 45
section 14 41
section 14(1) 40
section 14(2) 41
section 15 .... 167, 170, 244, 300
section 15(1) 68, 73
section 15(1)(a) 73, 147
section 15(1)(b) 74
section 15(1)(c) 76, 148
section 15(1)(c)(i) 76
section 15(1)(c)(ii) 77
section 15(1)(c)(iii) 77
section 15(1)(c)(iv) 77
section 15(2) 68, 78
section 15(3) 79
section 16 .... 65, 68, 82, 167, 183, 243, 278, 299
section 16(1) 82
section 16(2) 82, 83, 217
section 16(2)(a) 83
section 16(2)(b) 83
section 16(2)(c) 84
section 16(2)(d) 84
section 16(2)(e) 84, 90, 217
section 16(2)(f) 85, 217
section 16(2)(g) 85, 217
section 16(2)(h) 86, 217
section 16(2)(i) 86, 217
section 16(2)(j) 86, 88, 217
section 16(2)(j)(i) 87
section 16(2)(j)(ii) 87
section 16(2)(j)(iii) 88
section 16(2)(j)(iv) 88
section 16(3) 88, 167
section 16(4) 89, 92
section 16(4)(a) 90
section 16(4)(b) 90, 162
section 16(4)(c) 90
section 16(4)(d) 90
section 16(4)(e) 91
section 16(4)(f) 91
section 16(4)(g) 91
section 16(4)(h) 91
section 16(5) 91, 92
section 16(5)(a) 92
section 16(5)(b) 93
section 16(5)(c) 93
section 16(5)(d) 94
section 16(5)(e) 94
section 16(5)(f) 94
section 16(5)(g) 95
section 16(5)(h) 95
section 16(5)(i) 95
section 17 .... 65, 68, 98
section 17(1) 98
section 17(2) 98, 99
section 17(3) 99
section 18 .... 68, 102
section 18(1) 102
section 18(2) 103
section 18(3) 103
section 19 .... 65, 105, 230, 244
section 19(1) 69, 107
section 19(1)(a) 108, 111, 115
section 19(1)(b) 108
section 19(1)(c) 109
section 19(1)(d) 110, 162
section 19(1)(d.1) 110
section 19(1)(d.2) 111
section 19(1)(d.3) 111
section 19(1)(e) 112
section 19(1)(f) 112
section 19(1)(g) 113
section 19(1)(h) 113
section 19(1)(i) 113
section 19(1)(j) 113

section 19(1)(k) 114
section 19(1.1) 112
section 19(2) 69, 114
section 19(2)(a) 114
section 19(2)(b) 115
section 19(3) 68, 115
section 19(4)(a) 116
section 19(5) 116
section 19(5)(a) 116
section 19(5)(b) 116
section 20 .... 42, 69, 119, 167
section 20(1) 119
section 20(1)(a) 119
section 20(1)(b) 121
section 20(2) 120
section 20(3) 122
section 20(4) 122
section 21 .... 68, 124, 162
section 21(1) 124, 125, 126, 127
section 21(2) 126
section 21(2)(a) 126
section 21(2)(b) 127
section 21(2)(c) 127
section 22 .... 69, 130
section 22(1) 130
section 22(1)(a) 132
section 22(1)(b) 131, 133
section 23 .... 69, 124, 135
section 23(1) 135, 141, 142
section 23(1)(a) 135, 137
section 23(1)(b) 135, 138
section 23(1)(c) 135, 138
section 23(1)(d) 135, 139
section 23(1)(e) 131, 135, 139
section 23(1)(f) 135, 140
section 23(1)(g) 135, 140
section 23(1)(h) 135, 140
section 23(2) 141
section 23(2)(a) 141
section 23(2)(b) 141
section 23(2)(c) 142
section 23(2)(d) 142
section 23(2)(e) 142
section 23(2)(f) 143
section 23(2)(g) 143
section 23(3) 140
section 24 .... 69, 145
section 24(1) 145, 146, 147
section 24(1)(a) 145, 147
section 24(1)(b) 145, 147
section 24(1)(c) 145, 148
section 24(1)(d) 145, 149
section 24(2) 149
section 24(2)(a) 149
section 24(2)(b) 149
section 25 .... 69, 152
section 25(a) 152
section 25(b) 152
section 25(c) 152
section 26 .... 69, 153, 244
section 26(1) 153, 157
section 26(1)(a) 153, 154, 161, 162
section 26(1)(b) 153, 161
section 26(1)(c) 153, 155, 161
section 26(2) 68, 110, 153, 154, 161, 162
section 26(3) 153, 159
section 27 .... 69, 164
section 27(a) 164
section 27(b) 164
section 28 .... 69, 165
section 28(1) 165, 167
section 28(1)(a) 165
section 28(1)(b) 165, 166
section 28(2) 166
section 28(3) 166
Part 1, Division 3 167
section 29 .... 42, 45, 167, 170, 174, 221
section 29(1) 167, 168, 170
section 29(2) 167, 168
section 29(3) 169
section 29(4) 168, 170

section 30 ... 43

section 30(1) ... 170, 173

section 30(2) ... 171

section 30(3) ... 174

section 31 ... 68, 71, 179, 289, 291

section 31(1) ... 179, 183

section 31(1)(a) ... 181

section 31(1)(b) ... 182

section 31(2) ... 183

section 31(3) ... 183, 184

section 31(4) ... 184

Part 2 ... 4, 24, 29, 30, 166, 184, 185, 187, 188, 261, 262, 263, 265, 266, 273, 280, 283, 285, 288, 290, 291, 296, 301, 302

section 32 ... 189, 191, 267

section 32(a) ... 190, 267

section 32(b) ... 190, 267

section 32(c) ... 190, 200, 267

section 33 ... 273, 289

section 33(1) ... 192, 200, 267

section 33(1)(a) ... 192

section 33(1)(a)(i) ... 192

section 33(1)(b) ... 193

section 33(1)(b.1) ... 193

section 33(1)(b.2) ... 193

section 33(1)(b.3) ... 194

section 33(1)(b.4) ... 194

section 33(1)(c) ... 195

section 33(1)(d) ... 195

section 33(1)(e) ... 195

section 33(1)(f) ... 196

section 33(1)(g)(i) ... 196

section 33(1)(g)(ii) ... 196

section 33(1)(h) ... 197

section 33(1)(i) ... 197

section 33(1)(j) ... 198

section 33(1)(k) ... 198

section 33(2) ... 199, 200, 213, 274

section 33(3) ... 200, 267

section 34 ... 201

section 34(a) ... 201, 202, 269

section 34(b) ... 65, 202, 289

section 35 ... 188, 204, 269

section 35(1) ... 203, 288

section 35(1.1) ... 204

section 35(2) ... 205

section 35(3) ... 207, 216

section 35(3.1) ... 207

section 35(4) ... 207

section 35(5) ... 207

section 35.1 ... 40, 208, 300

section 35.1(2) ... 41

section 36 ... 208, 209, 270, 277

section 37 ... 210, 211, 272, 273

section 37(1)(a) ... 211, 212

section 37(1)(b) ... 211, 212

section 37(1)(c) ... 211, 213

section 37(2) ... 211, 214, 237

section 37(3) ... 214

section 37(4) ... 214

section 38 ... 183, 210, 213, 215, 216, 272, 273, 289

section 38(1) ... 243

section 38(1)(a) ... 216

section 38(1)(a.1) ... 217, 243

section 38(1)(aa) ... 235, 295

section 38(1)(b) ... 219, 238

section 38(1)(bb) ... 236

section 38(1)(cc) ... 236

section 38(1)(d) ... 221, 222, 231

section 38(1)(dd) ... 236

section 38(1)(e) ... 222

section 38(1)(f) ... 223

section 38(1)(g) ... 223, 224

section 38(1)(g.1) ... 224, 237

section 38(1)(h) ... 225

section 38(1)(i) ... 225

section 38(1)(j) ... 226

section 38(1)(k) ... 227

section 38(1)(l) ... 228

section 38(1)(m) ... 229

section 38(1)(n) ... 229

section 38(1)(o) 230
section 38(1)(p) 231
section 38(1)(q) 231
section 38(1)(r) 232
section 38(1)(s) 232
section 38(1)(t) 232
section 38(1)(u) 233
section 38(1)(v) 233
section 38(1)(w) 233
section 38(1)(x) 234
section 38(1)(y) 234, 236
section 38(1)(z) 234
section 38(1.1) 236
section 38(1.2) 237, 272
section 38(2) 214, 215
section 39 .... 212, 237
section 40 .... 83, 243, 272
section 40(a) 239
section 40(b) 240
section 40(c) 240
section 40(d) 241
section 41 242
section 41(1) 242, 245
section 41(1)(a) 243
section 41(1)(a) (i) 243
section 41(1)(a) (i)(A) 243
section 41(1)(b) 244
section 41(2) 242, 245
Part 3 .... 287, 295
section 43 287
section 44 287
section 45 287
section 51 .... 29, 30, 184, 287, 301
section 51(1) 288, 301
section 51(1)(a) 250, 288
section 51(1)(b) 288
section 51(1)(c) 288
section 51(1)(d) 288
section 51(1)(e) 288
section 51(1)(f) 288
section 51(1)(g) 288
section 51(1)(h) 192, 288
section 51(1)(i) 288
section 51(1)(j) 288, 290
section 51(2) 296, 300, 301, 308
section 51(2)(a) 288
section 51(2)(b) 288
section 51(2)(d) 288
section 51(2)(e) 288, 301
section 52 291
section 52(1) 290
section 52(2) 291
section 53 .... 36, 37, 292
section 54 298
section 54(1) 291, 292
section 54(2) 291, 292
section 54(3) 292, 298
section 54(4) 292, 298
section 54(5) 292, 298
section 55(1) 294
section 55(2) 294
section 56 294
section 57 294
section 57(2) 294
section 57(3) 294
section 57(4) 294
section 57(5) 294
section 58 295
section 59(1) 295
section 60 289
section 61 .... 29, 289
Part 4 .... 30, 291
section 62 .... 295, 301
section 62(1) 53, 55, 65, 173, 184, 295
section 62(2) 295
section 62(3) 295, 301
section 62(3.1) 295
section 62(4)(b) 153, 159
section 63 296
section 63(2) 173
section 63(2)(a) 296, 302
section 63(2)(b) 296, 302

section 64 300
section 64(1) 297
section 65 297
section 66 298
section 66(2) 298
section 66(3) 298
section 66(4) 298
section 66(5) 298
section 66(6) 299
section 66.1 299
section 67 299
section 67(1) 299
section 67(2) 299
section 67(3)(a) 300
section 67(3)(b) 300
section 68 .... 29, 300
section 68(3) 288
section 68(3)(b) 45
section 68(4) 300
section 68(6) 301
section 69 .... 289, 300
section 70(1) 300
section 70(4) 300
section 71 .... 287, 302
section 71(1.1) 302
section 73(1) 173
section 74(1) 302
section 74(2) 173
section 76 303
section 76(2) 29
section 77 29
section 77(1) 184, 291
section 77(2) 185, 291
section 77(3) 185
section 77(4) 185
section 77(5) 185
section 77(6) 185
section 77(7) 185, 291
section 78 .... 50, 168
section 79 .... 83, 246
section 79(1) 17, 221
section 79(1)(a) 246
section 79(1)(b) 247
section 79(1)(b.1) 247
section 79(1)(c) 247
section 79(1)(d) 247
section 79(1)(e) 248
section 79(2) 248
section 80 26
section 81 27
section 82 .... 28, 246
section 82(1) 31
section 82(2) 31
section 82(3) 31, 212, 216, 245
section 82(4) 274
section 82(5) 32
section 82(6) 32, 255
section 82(9) 31
section 83 244
section 83(1) 16
section 84(1) 32, 143
section 84(2) 33
section 85 29
section 85.1 29
section 85.1(1) 30
section 85.1(2) 30
section 86 .... 29, 294
section 86(1) 29, 30, 280
section 86(1)(c.1) 48
section 86(1)(e) 48, 210
section 86(2) 30, 280
section 87 .... 50, 51, 52, 55, 296
section 87(1) 50, 51
section 87(2) 50
section 87(3) 51, 52
section 87(4) 51, 52, 54
section 87(4.1) 55, 289
section 89(a) 23
section 89(c) 51

Freedom of Information and Protection of Privacy Regulation

schedule 1 .... 1, 24, 140
schedule 2 .... 51, 52
section 1(3) 309
section 1(4) 312
section 2 .... 38, 87
section 2(1) 31
section 2(3) 39
section 3 64
section 4 34
section 5 .... 99, 232
section 5(5) 99
section 6 .... 212, 220
section 7 227
section 10 51
section 11 52
section 12 52
section 13(1)(b)... 54
section 13(2) 54
section 13(3) 54
section 15 72
section 15(2) 72
section 16 72
section 17 72
section 18 131

Index of

Information and Privacy Commissioner's Order and Investigation Report Citations

Information and Privacy Commissioner's Order and Investigation Report Citations

Investigation Report 98-003 .... 191, 209, 210
Investigation Report 98-009 ....47, 251
Investigation Report 98-011 ....180, 183
Investigation Report 99-001 ....11, 189
Order 96-003..................................76, 108
Order 96-006...137
Order 96-007..230
Order 96-009...158
Order 96-011.................................182, 184
Order 96-013....................................73, 74
Order 96-015............. ....154, 155,156, 157, 161, 292
Order 96-017......... ....70, 71, 154, 155, 156, 157, 158, 161
Order 96-018...77
Order 96-019..................................61, 155
Order 96-020............. ....153, 154, 156, 157, 158, 159, 160, 161, 162
Order 96-021............. ....92, 155, 156, 157, 158, 160, 162, 251
Order 96-022.....................................47, 48
Order 97-001...55
Order 97-002.....................................92, 95
Order 97-003.............................14, 36, 153
Order 97-007...................................13, 137
Order 97-008...9
Order 97-009.............................4, 156, 180
Order 97-010...128
Order 97-013...75
Order 97-017...................................12, 153
Order 97-018.................................168, 182
Order 97-019...................................52, 251
Order 97-020...........................60, 205, 206
Order 98-001.........................204, 235, 300
Order 98-002......................18, 41, 191, 202
Order 98-003...251
Order 98-004............. ....85, 90, 92, 95, 155, 157, 165, 246
Order 98-005 .... 60, 149
Order 98-007 .... 72, 84, 94
Order 98-008 93
Order 98-009 .... 65, 96
Order 98-010 .... 205, 206, 300
Order 98-011 252
Order 98-013 .... 13, 73
Order 98-014 86
Order 98-016 60
Order 98-017 157
Order 98-018 86
Order 98-019 .... 13, 182
Order 98-020 .... 68, 148
Order 98-021 102
Order 99-001 .... 137, 138
Order 99-002 .... 60, 251
Order 99-005 13
Order 99-007 75
Order 99-009 252
Order 99-010 .... 109, 110, 159
Order 99-011 .... 34, 38, 299
Order 99-014 .... 51, 59
Order 99-020 60
Order 99-021 .... 62, 251
Order 99-025 .... 7, 8
Order 99-032 .... 6, 11, 223
Order 99-034 72
Order 2000-005 .... 6, 74, 75

Index of

Words and Phrases Discussed or Defined

Words and Phrases Discussed or Defined

ability to manage the economy 146
aboriginal organization 120
aboriginal people 94
abuse of the right of access 293
access 307
active dissemination 16
activity (section 16(2)(j)) 88
activity (section 32(c)) 191
adjudicative function 141
adjudicator 307
administration of a public body 139
administrative investigation 106
advice 137
advice and recommendations (section 21) 126
advice and recommendations (section 23) 137
agreement (section 38(1)) 221
allied state 109
analyses or policy options 137
annotate (correction of personal information) 205
applicant 307
applicant's rights 93
arbitrator 78
archives of a public body 243
arrangement (section 38(1)) 221
assist in resolving a problem (disclosure to MLA) 228
associated state 109
associations (section 16(4)) 91
audit 140
audit purposes (section 38(1)) 227
auditor general 227
available for purchase by the public 165
background facts 127
background research 142
bad faith 185
benefits (section 18) 102
benefits derived (research) 240
burden of proof 307
by-law 130
Cabinet 307
claims, disputes or grievances 94
class privileges 154
clearly in the public interest 182
collected for the purpose of collecting a tax 78
collected for the purpose of determining tax liability 78
collection 189
commercial information 74
commissioner 307
committee of a governing body 131
committees of the Executive Council 125
common program or service 224
compelling circumstance (section 16) 84
compile (personal information) 212
complaint 308
comply with a treaty, arrangement or agreement (section 38(1)) 221
comply with an enactment (section 38(1)) 221
confidential source 110
confidentiality (section 40) 241
consistent use (personal information) 212
constituency records 11
consultation 308
consultations or deliberations 138
continuing request 308
contract to supply goods and services 85
contracts 102
control 6, 308
correctional record 114
criminal intelligence 105
criminal intelligence operations 110
Crown privilege 160
Crown records (privileged information) 160
custody 6, 308
damage (section 27) 164

damage the reputation 95
data linkage 281
data matching 281
data profiling 281
data sharing 281
day of response 45
debt 195
decision that directly affects the individual 201
deemed waiver (privileged information) 157
defence of Canada 108
delegation 308
deliberation 125, 138
determination of benefit levels 90
directory of records 308
disclose 215
disclosure 309
discretion 309
discretionary benefit 86
discretionary benefit of a financial nature 86
dominant purpose 156
draft 130
draft legislation or regulations 126
economic interests 145
educational body 2
every reasonable effort (section 34) 202
elected officials 131
eligibility 90
employee 223, 309
employment 102
enactment 309
endangered form of life 164
error (section 35) 204
espionage 109
ethnic origin 91
every reasonable effort 41
exceptions to disclosure 309
exercise of discretionary power 141
explicitly in confidence 75
expressly authorized by an enactment (section 32(a)) 190
extension 309
factual information (section 35) 204
fair determination of rights 93
fair trial 112
fees 310
fifteen years 133
financial information 74
financial interests 146
financial loss 148
fine 195
FOIP 310
foreign state 120
formal 140
Freedom of Information and Privacy Coordinator 310
frivolous or vexatious 37, 293
gathered for the purpose of collecting a tax 91
good faith 184
governing body 12, 310
government of Alberta (section 15) 79
government of Alberta (section 24) 145
guardian 247
harm 69, 310
harm (law enforcement) 108
harm (section 40) 240
harm to health 181
harm to safety 181
harm to the environment 181
has been implemented 127
head 310
health care body 2
historic resources 164
history (section 19(2)) 115
history (section 33(1)(e)) 195
identifiable individual 82
identified (personal information) 220
identity 110
immediate and grave harm 99
imminent danger 236

impartial adjudication 112
implementation 139
implicitly in confidence 75
in a reasonable manner (use and disclosure of personal information)... 214
in confidence 75, 310
in the absence of the public 132
inaccurate information 201
incomplete 140
individually identifiable form (personal information) 239
information collected on a tax return 78
inquiry 311
integrated program or service 224
interfere with 111
interfere with contractual or other negotiations 149
interference with public safety 98
international organization of states 120
investigation 105
investigative techniques and procedures 109
judicial administration record 7, 311
judicial review 289, 311
labour relations 74
labour relations officer 78
law enforcement 105, 311
law enforcement agency (section 38(1)) 230
law enforcement proceeding 231
law enforcement record 115
lawfully detained 113
lead or could lead 105
legal advice 155
legal proceedings 312
legislative authority 231
licence 85
limited waiver (privileged information) 158
link (correction of personal information) 205
litigation privilege 156
local government body 2
local public body 2, 312
management of personnel 139
management or administration of personnel (sections 33(1) and 38(1)) 198
matching program 282
matching recipient 282
matching source 282
mediator 78
meeting 312
meeting (section 22) 131
member of the Executive Council 224
member of the Legislative Assembly 228
mental health 98
Minister responsible for the Act 312
monetary value 148
necessary for (section 32(c)) 191
necessary for (section 39) 238
non-arm's length transaction (section 4(1)(m) and (n)) 13
non-arm's length transaction 312
notice 312
offence 313
offence under an Act of Canada 115
officer 223
Officer of the Legislature 313
omission (section 35) 204
operating program 191
opinions (section 35) 204
order 313
order (section 38(1)) 223
organized criminal activities 111
other details (contracts) 85
other persons or bodies (labour relations) 78
other public sources (section 33(1)) 194
parliamentary privilege 159
participant 103
peace officer 113
penalty or sanction 106
permit 85
person 112

personal information 313
personal information bank 31, 313
personal note 7
personal service (section 29) 169
physical health 98
police informer privilege 158
police investigation 106
policing 105
policy considerations 126
positions and plans 138
post-secondary educational body 10
prejudice (section 19) 108
prejudice to competitive position 148
prescribed 313
privacy impact assessment 262
private records (privileged information) 160
procedures, criteria, instructions and considerations 139
proceedings 107
program contact 25
progress 141
prohibition on disclosure (research) 241
proposals 137
proprietary interest 148
protection of the environment 93
provincial public body 313
public body 1, 314
public event 88
Public Guardian 197
public health 93
public interest (section 16(2)(j)) 87
public interest (section 31) 182
public interest (section 40) 240
public interest immunity (privileged information) 160
public interest privilege 154
public safety 93
Public Trustee 197
published sources (section 33(1)) 194
purpose (collection of personal information) 219
purpose (use of personal information) 211
quality assurance committee 314
racial origin 91
rare form of life 164
reasonable 314
reasonable and direct connection 238
reasonable security arrangements (section 36) 208
reasonably be expected to 315
reasons 141
record 5, 315
record linkage (section 40) 240
record of a credit union 315
recorded (personal information) 82
records retention and disposition schedule 315
records system 255
relate (section 16(4)) 90
relates directly to (section 32(c)) 191
relations (section 20) 119
release (section 33(1)e)) 196
released to the public 166
relevant and material (correction of personal information) 206
relevant circumstances (section 16(5)) 92
religious or political beliefs 91
removal or destruction of individual identifiers 241
repetitious 36
report (labour relations) 78
request 315
research information (post-secondary educational body employees) 9
research purpose 239
resolution 130
retain (section 34) 203
review 315
risk (section 31) 181
routine disclosure 16
sabotage 109
safety 98
scientific information 74

scope 315
security 114
security impact assessment 262
security investigation 106
serious and repetitive criminal
 activities..111
severing 315
solicitor–client privilege 154
statistical research 239
statistical surveys 142
statistics...142
subpoena 223
substance 125
substitutional service..............................169
suitability 226
supervision 115
supervision (correctional authorities)....196
systematic...36
teaching materials 9
technical information 74
terrorism 109
test..152
third party 74, 167, 315
threaten..98
threatened form of life 164
time limit..316
trade secret 73, 316
transfer 316
transitory record 316
treaty 221
unauthorized access (personal
 information)......................................209
unauthorized collection (personal
 information)......................................209
unauthorized destruction.......................210
unauthorized disclosure (personal
 information)......................................210
unauthorized use (personal
 information)......................................210
unreasonable interference with the
 operations of a public body 293
use (personal information) 211
validating 94
vulnerable form of life.......................... 165
warrant 223
without delay 179

Subject index

Subject Index

A

aboriginal organizations
  intergovernmental relations ... 119
aboriginal people
  claims, disputes or grievances ... 94, 198
  negotiations ... 120
absenteeism reports ... 91
academic councils ... 12, 131
Access Request Review Form ... 391
  Detailed Review of Records Form ... 391
Access Request Review Recommendation/Summary Form ... 391
access requests ... 64
  adequacy of search ... 250–53
  consultations
    third parties ... 167–76
  disregarding ... 292–94
  documenting ... 58
  evading ... 29
  forms ... 391
  personal information ... 216
  processing ... 46–65
  prosecutions ... 116
  records excluded from *FOIP Act* ... 64
  records issues ... 250–53
  refusal of access ... 61, 62, 64, 339-41, 342, 343
  refusal to confirm or deny existence of records ... 63, 343
  responding to ... 14–21, 61, 62–65
  severing ... 59–62
access rights ... 1, 34, 67, 70
  abuse ... 36, 292
  defined ... 31
  limitations on ... 67
access to information ... 31–66
  existing procedures ... 4, 14
  methods ... 31–66
***Access to Information Act* (Canada)** ... 73
access tools ... 31–33
accountability ... 1, 92
accountants
  audits ... 228
accuracy, *see* **personal information**, accuracy
active dissemination ... 16–18, 20, 166
  communications ... 19
  copies of records ... 62
  delegation of authority ... 19
  Internet ... 16
  records management ... 257
activities, *see* **public events**
Acts of Alberta
  collecting personal information ... 190
  disclosing personal information ... 221–23
    restrictions ... 244
  disclosing third party information ... 79
  routine disclosure ... 16
Acts of Canada
  collecting personal information ... 190
  disclosing personal information ... 221–23
    restrictions ... 244
  disclosing third party information ... 79
  offences ... 115
  routine disclosure ... 16
addresses
  personal information ... 5
adjudication and adjudicators ... 287
  FOIP Act ... 302–3
  impartiality ... 112
  Information Management and Privacy ... 303
  judgments
    reasons for decision ... 141
  reviews ... 42
administration
  public bodies
    plans ... 139
Administrative Procedures Act ... 7
administrative proceedings
  law enforcement ... 107
administrative records disposition authority ... 65
admissions
  hospitals ... 87, 218
  nursing homes ... 87, 227
advice
  defined ... 137
  Executive Council ... 126
  Information and Privacy Commissioner ... 290–91
  legal matters ... 154, 155, 223
  officials ... 134–44
    records 15 years old ... 141
Affidavit for Witness Form ... 391

- **age**
  - personal information 5
- **agencies** 1, 24
  - agenda or minutes 140
  - intergovernmental relations 119
- **agenda**
  - consultations or deliberations 138
  - Executive Council 125
  - *in camera* meetings 132
  - public bodies 140
- **Agenda and Priorities Committee** 125
- **agents**
  - collection of personal information 189
  - *Personal Directives Act* 247
- **Agreement for Access to Personal Information for Research or Statistical Purposes Form** 391
- **agreements**
  - disclosing personal information 221
    - contents of 222, 240–42
    - research 240–42
  - expert consultations 232
  - law enforcement 231
  - use of alumni records 236
- **air quality**
  - testing 142
- **Alberta Cancer Board** 2
- **Alberta Community Development** 28
- **Alberta Energy and Utilities Board** 8
- ***Alberta Evidence Act***
  - section 9 8
- **Alberta Health and Wellness** 28, 222
- **Alberta Health Care Insurance Regulation** 192
- **Alberta Health Facilities Review Committee** 158
- ***Alberta Housing Act*** 3
  - section 37 3
  - section 38 3
- **Alberta Infrastructure** 236
- **Alberta Innovation and Science** 65, 211, 256
  - records management 249
- **Alberta International and Intergovernmental Relations** 28, 121, 122
- **Alberta Justice** 28, 197, 225, 232
  - adjudication and adjudicators 303
  - as law enforcement agency 230
  - prosecutions 112
  - protocols
    - disclosure of personal information 181
- **Alberta Learning** 28
- **Alberta Municipal Affairs** 24, 28, 39, 40, 72
  - disclosure harmful to intergovernmental relations 121
  - Information Management and Privacy Branch, *see* **Information Management and Privacy**
- **Alberta Records Centre** 203, 251
- **Alberta Records Management Committee** 65, 203, 210, 211, 258
- **Alberta Securities Commission** 230
- **Alberta Seniors Benefit** 196, 222
- **Alberta Treasury**
  - processing fees 54
  - Treasury Board records 124
- **Alberta Treasury Branch** 13
- ***Alcohol and Drug Abuse Act*** 242
- **alliances** 109
- **alumni records**
  - fund-raising 214, 236
  - post-secondary educational bodies 214, 236
- **ambulances**
  - patients 87
- **analyses**
  - advice and recommendations 137–38
- **appeals**
  - Executive Council 127
- **applicants**
  - assisting 24, 34, 59, 60, 64, 288
  - burden of proof 299
  - harm to health or safety 98, 232
  - identities 46, 168, 170
  - notices 170, 326–43
  - proof of identity 17, 63
  - refusal to disclose own personal information 98, 101–4
  - responding to 61, 62–65, 72, 296, 326–43
  - rights 93
    - fee waivers 55
    - reviews 295–302
- **appointment books**
  - elected officials 11
  - governing bodies 12
- **arbitrators** 78
  - reports 77
- **archaeological resources** 164

archives
  75-year-old records 244
  church records 10
  disclosing business information 80
  disclosing personal information to 229–30
  disclosure of personal information 242–45
  information 25 years old 244
  labour union records 10
  policies and procedures 245
  post-secondary educational bodies 242–45
  private records 10
  records excluded from the *Act* 10
  transfer of records to 48, 210, 229, 242, 244, 251, 258
  unrestricted records 4, 242
arrangements
  disclosing personal information 221
  law enforcement 231
assessment, *see* **property**, assessment information
Assessment Review Boards 8
  reasons for decision 141
assets
  public bodies 146
  verification of 196
associations
  personal information 5, 91
atmosphere
  harm to 181
Attendance Boards 106
Attorney General, *see* **Minister of Justice and Attorney General**
audio tapes 194, 209
Auditor General 227
  disclosing personal information to 234
  office 2
  records excluded from *FOIP Act* 8
Auditor General of Canada 227
audits
  disclosure of personal information for 227–28
  electronic records 257
  harm to 152
  incomplete 140–41
  Information and Privacy Commissioner, *see* **Information and Privacy Commissioner**, audits
  methods and procedures 152
  personnel management 152, 228
  privacy 264, 302, 371–77
  routine disclosure 19
  tax 79
Authorization of Representative Form 391
awards 102
  receipt of 88, 219
  suitability for 194

B

background facts
  defined 127
  Executive Council or Treasury Board 127–28
  not advice 137
  reports to be published 165
  scientific 142
  technical 142
bad faith 185
bail 114, 115, 196, 234
bailiffs 102
Banff Centre Act 2
banking records 13
bankruptcy 79
bargaining agents
  disclosing personal information to 229
bargaining positions 138
benefits
  confidential evaluations 101–4
  continuing eligibility for 197
  denying 213, 240, 284
  determination of levels 90
  eligibility 90, 196–97, 226–27
bills, drafts of 139–40
biometrics 262
blood type 5
Board of Reference 8
boards 1
  agenda or minutes 140
  appointees 84, 235
boards of governors 12, 131
bombs
  technical information 113
  threats 181
books 5
briefing materials or notes
  Executive Council or Treasury Board 126
  solicitor's 156

brochures
  collection of personal information...... 199
budgets 146
  pending decisions 140
  third parties 74
buildings, *see* **property**
burden of proof 299–300
  confidential information 94, 121
  disclosing personal information... 89, 299
  third parties 300
bursaries 194, 219
business plans 74, 139
businesses
  budgets.. 74
  client records 74
  financial gain 77
  financial loss 77
  harm 73–81
  information
    50 years old 80
    revealed 73
  licences and permits..................... 85, 217
  personnel management 74
  records 73–74
  tax information 78
by-laws
  drafts 130
  law enforcement 106
    personal information 90
  local public bodies 5, 131
  municipal 90
  routine disclosure.................................. 16

C

Cabinet confidences 124–29
  records
    15 years old 126
    5 years old 128
Cabinet ministers, *see* **ministers**
calendars
  elected officials...................................... 11
  governing bodies 12
  post-secondary educational
    bodies 199, 218
**Canadian Security Intelligence
  Service**... 122
Canadian Standards Association......... 187
case-by-case privilege..................... 160–61
catalogues.. 165
Charitable Fund-Raising Act 223
charter schools...................................2, 87
cheating
  administrative investigations 107
Check Stop programs 116
Chief Electoral Officer
  disclosing personal information to......234
  office 2
  records excluded from *FOIP Act* 8
Chief Justice of Alberta 303
Child and Family Service Authorities .225
Child Welfare Act 242
children, *see* **minors**
children's services 225
churches
  archival records.....................................10
  membership...91
civil actions, *see* **legal matters**, civil legal
  cases
civil liability
  discretionary exceptions 114
class privileges 154–59
class reunions...............................87, 218
client records
  businesses 74
  economic interests of public bodies.... 148
  routine disclosure............................17–18
clients
  surveys 199
**code of fair information
  practices**........................ 187–89, 261–86
collection agencies 225
**collection of personal
  information**................ 189–201, 267–69
  agreements between public bodies 189
  audits...371–73
  collecting fines or debts 195
  consent to indirect collection 192
  contracts and contractors 190
  correctional authorities or
    institutions 195
  direct 192, 267–69
  emergencies 193
  forms 199, 274–77
  from Internet 194
  from other public bodies......................193
  fund-raising..194
  honours or awards................................194
  indirect 192–99
  interviews...................................189, 199
  investigations 195, 301
  law enforcement..........................190, 195

  legal matters 196
  legal proceedings 196
  limitations on 190
  literacy programs 201
  maintenance enforcement 197
  means of collecting 189
  methods 192–201, 267–69
  notices 199–201, 267–69, 274–77
    exceptions 200
  personnel management 198
  programs and services 190
  provision of legal services 196
  purposes 189–92, 212, 237
  registries 11
  review of practices 191
  unauthorized 209
  verifying eligibility for programs or services 196–97
collective agreements 74
colleges 2, 10, 90
  enrolment 87
  reunions 87, 218
Colleges Act 2
colour
  personal information 5
commercial information 74, 147–48
commissions 1
  agenda or minutes 140
committees
  appointees 84
  governing bodies 131
  interdepartmental 40
  standing 125
common programs or services, *see* **programs and services**, common programs
communications
  Cabinet decisions 127
  information dissemination 19
  solicitor–client 154–56
  strategies 25
communications systems
  security 113, 279
Community Development, Department of, *see* **Alberta Community Development**
community health councils 2
community library boards 3
community service work 115, 196, 234
competitive position
  harm 76
  public bodies 148
complaints 288, 301
  duty to assist 296
  extension of time limits 296
  fees 296
  law enforcement 108
    investigations 105
  personal information correction 296
  personal information banks 32
  time extensions 45
  time limits 302
  violation of Part 2 296
computers
  security 106, 113–14, 209, 258, 278–79
confidential information
  administrative investigations 107
  Cabinet and Treasury Board 124–29
  complaints
    law enforcement 108
  confidential sources 110
  correctional records 114
  employment 101–4
  Executive Council 124–29
  explicit 75
  identity of source
    health or safety threats 99
  implicit 75
  intergovernmental relations 119–23
  law enforcement 110
  local government bodies 119–23
  local public bodies 130–34
    records 15 years old 133
  public interest privilege 154
  solicitor–client communications 155
  third parties
    private records 160
  third party business 74–75
  unreasonable invasion of privacy 94
  voluntarily supplied 75
confidential sources, *see* **confidential information**, confidential sources
conflicts of interest
  Ethics Commissioner 9
  Information and Privacy Commissioner 287, 302–3
Conflicts of Interests Act 9
consent
  collecting personal information .. 192, 196
  disclosing confidential information
    intergovernmental relations 122

  disclosing personal information 83, 220, 228
  disclosing third party information 79, 170–71
  disclosure harmful to intergovernmental relations 120–21
  disclosure of privileged information 153
  exercise by other persons 83
  forms 391
  police informer privilege 158
  using personal information 212
conservation
  endangered forms of life 164–65
  historic resources 164–65
conservation officers 230
consistent purpose, *see* **personal information**, consistent use
consistent use, *see* **personal information**, consistent use
constituency records 3, 11, 12
consultants, *see* **contracts and contractors**
consultations
  economic interests of public bodies 146
  FOIP requests 40, 41, 42, 49, 167
  historic resources 164
  intergovernmental relations 122
  officials 138
  privileged information 153
  third parties 42, 167–76
    public interest 183–84
contaminants 181
contempt of court 223
  Information and Privacy Commissioner 291, 298
continuing FOIP requests 35–36
  fee estimates 52
  fees 51
  notices 329
  tracking 35
Contract Manager's Guide, *see* ***Freedom of Information and Protection of Privacy: Contract Manager's Guide***
contracts and contractors
  advice and recommendations 137–38
  audits 227
  collecting personal information 189, 190
  confidential evaluations 101–4
  disclosing personal information 85, 217
  disclosure of personal information to employees 223–25
  employment contracts 85, 217
  FOIP Act 7
  goods and services 85, 217
  negotiations 138–39, 149
  personal information 84, 217
    security 209, 377
  personal information systems 266
  personal service contracts 85, 139, 198, 217
  privacy protection 189
  records 6–7, 259
    retrieval 47
    routine disclosure 19
  research reports 141
  security 280
  terms and conditions of contracts 85, 217
  trade secrets 147
control 6–7
  law enforcement records 105
Coordinated Law Enforcement Unit 230
coordinating committees
  information dissemination 19
***Copyright Act* (Canada)**
  section 32.1 72
corporations 1
  agenda or minutes 140
  archival records 10
  banking records 13
  disclosure harmful to personal privacy 82
  registry records 10
correction of personal information, *see* **personal information**, correction
correctional authorities or institutions
  collecting personal information 195
  disclosing personal information to 233, 234
  escape from 113
  individuals under the supervision of 114
  inmates
    legal representatives 236
  records 114
correctional officers 113
correspondence 5
  elected officials 11
  governing bodies 12
  Minister of Justice and Attorney General 153, 161
  ministers 12, 125
  MLAs 12
  Officers of the Legislature 8
  Secretary to Cabinet 126

cost–benefit analysis
  data matching 284
  privacy impact assessments 264
counselling records 6
  personal information 90
  retention 202
course evaluations
  post-secondary educational bodies 237
Court of Appeal of Alberta
  excluded from *FOIP Act* 3
  records 7
Court of Queen's Bench of Alberta
  excluded from *FOIP Act* 3
  records 7
court records 3, 7
Credit Union Act
  records 13
  section 119(3) 13
Credit Union Central Alberta Limited . 13
Credit Union Deposit Guarantee Corporation 14
credit unions
  records 13
crime prevention 105, 113, 116
Crimestoppers programs 116
criminal acts
  commission of 113
  disclosure contrary to public interest 87, 218
  organized 111
  serious and repetitive 111
***Criminal Code* (Canada)** 90, 111, 115
criminal history
  correctional records 114
  disclosure in public interest 181
  personal information 5
criminal intelligence 105, 110–11
criminal records, *see* **criminal history**
Crown records 160
CSIS, *see* **Canadian Security Intelligence Service**
custody 6–7
  law enforcement records 105
customer records, *see* **client records**

D

damage, *see* **harm**
data
  encryption 209, 262
databases
  information dissemination 18
  licensing 20
  local public bodies 18
  matching 240, 265, 273, 281–86, 375
  personal information 261
  routine access 15
  sharing 265, 273, 281–86
deaf, *see* **hearing-impaired persons**
debts
  collection of personal information 195
  disclosure to collect 225–26
  securing 10
deceased individuals
  disclosure not unreasonable invasion of privacy 235
  disclosure of personal information 232, 235–36, 246
  more than 25 years deceased 86, 217, 243
  privacy 86, 217
    reviews 295
  proof of death 235
  relatives 235
  reputation 94
deemed refusal 42
defence
  Canada 108–9
degrees 219
  honorary 194
delegation of authority 26–27
  routine disclosure 19, 26
delegation orders 26–27
delegation table 26, 319–25
deliberations
  officials 138
  substance of 124, 125
    local public bodies 130–34
Department of National Defence 120
dependent adults 197
Dependent Adults Act 223, 247
deputy ministers
  disclosure statements 9
design specifications 74
detriment, *see* **harm**
development permits 85
diagnostic and treatment information, *see* **health care**, personal information
diaries 160

direct collection, *see* **personal information**, direct collection; **collection of personal information**, direct
Director of Maintenance Enforcement 234
directories, *see* **records**, directories of holdings; **personal information banks**, directories
disabled persons
  FOIP requests 34
  transportation 218
disasters, *see* **emergency planning**
disclosure
  advice from officials 134–44
  by Information and Privacy Commissioner 294
  communications strategies 25
  copyright material 73
  emergencies 84
  employee information 84–85
  exposure to civil liability 114
  harm to economic and other interests of public bodies 145–51
  harm to health or safety 98–101
  harm to historic resources 164–65
  harm to intergovernmental relations 119–23
  harm to law enforcement 105–18
  health or safety danger 83–84
    notices 361
  historical practices 71
  individual under supervision of correctional authority 114
  information 25 years old 244
  labour relations information 77–78
  licences and permits 85–86, 217
  mandated by Act or by-law 16
  negotiations 138–39
  not unreasonable invasion of privacy 82–89, 167, 217–19, 243
  personal information 82–96, 215–37, 238–48, 272
    archival purposes 229–30, 242–45
    audits 227–28, 374–75
    collecting fines or debts 225–26
    common programs and services 224–25
    compliance with enactments 221–23
    compliance with subpoena, warrant or order 223
    consent 83, 220, 228, 229
    consistent use 219
    constraints
      law enforcement 231
    constraints on 215, 225, 240
    correctional authorities or institutions 233, 234
    court proceedings 232–33
    deceased individuals 235–36, 246
    defined 215
    discretionary benefits 85–86
    emergencies 231
    enforcing legal rights 225
    expert consultations 232, 366–67, 368
    for investigations 90, 230–31
      forms 391
    guardians 247–48
    Internet 235
    judicial tribunals 232–33
    labour unions 229
    law enforcement 230–31
    legal matters 225
    legal proceedings 225, 232–33
    maintenance enforcement 233
    making payments 225–26
    minors 247–48
    not contrary to public interest 86–89, 217
    Officers of the Legislature 234
    original and consistent use 219
    pastoral care 218
    personnel management 233
    proof of identity 17, 63
    public events 88
    public health 92–93
    public information 234–35
    public interest 92–93
    public safety 92–93
    public scrutiny 92
    quasi-judicial proceedings 232–33
    quasi-judicial tribunals 232–33
    record of purposes 246, 273
    records of 216
    refusal of consent 220
    research agreements
      contents of 240–42
    research purposes 84, 238–45, 272–73
    restrictions on archives 244
    statistical purposes 238–45, 272–73
    to avert imminent danger to health or safety 236
    to bargaining agents 229

    - to Information and Privacy Commissioner 234
    - to employees 223–25
    - to ministers 223–25
    - to MLAs 228
    - to Ombudsman 234
    - to representatives 246–48
    - unauthorized 210, 216
    - use after disclosure 193, 213–14
    - vehicle accidents 236
    - verifying eligibility 226–27
  - policies 70
  - privileged information 153–63
  - protection of environment 92–93
  - public interest 178–85, 216
    - notices 183, 359, 360
  - published information 165–66
  - records excluded from *FOIP Act* 14
  - research purposes 232
  - tax information 78–79
  - third party information
    - consent 79, 221
  - to Information and Privacy Commissioner 184–85, 291
  - unreasonable invasion of privacy 89–96, 247–48
    - determining 91–95

- discovery, *see* **examination for discovery**
- **discretion**
  - exercising 70–72
- **discretionary benefits**
  - disclosure
    - not unreasonable invasion of privacy 85–86, 217
  - employees 85, 217
- **discretionary exceptions** 68–72
  - advice from officials 134–44
  - civil liability 114–15
  - confidential evaluations 101–4
  - exercising of discretion 70–72
    - advice from officials 136
  - harm to economic and other interests of public bodies 145–51
  - harm to historic resources 164–65
  - harm to law enforcement 105–18, 244
  - harm to public or individual safety 98–101
  - individual under supervision of correctional authority 114–15
  - intergovernmental relations 119–23
  - local public body confidences 130–34
  - notices 339–41
  - privileged information 153–63, 244
  - published information 165–66
  - routine disclosure 16
  - severing 60
- **discretionary powers**
  - reasons for decision 141
- **district registrars** 10
- DNA, *see* **inheritable characteristics**
- **documentation**
  - line-by-line review of records 58, 61
- **documents** 5
  - creation for ease of severing 61
  - drafts
    - transitory records 256
- **dog licences** 86
- ***Drainage Districts Act*** 3
- **drawings** 5
- **drugs**
  - criminal acts 111
  - testing procedures 74, 150
  - tests 142
- **duty to assist** 24, 34, 59, 288
  - investigations 301

E

- **economic development agencies** 120
- **economic interests**
  - harms test 145–46
  - public bodies 145–51
- **education**
  - personal information 5, 90
- **educational bodies** 2
  - administrative investigations 107
  - head 23
  - tax information 78
  - testing procedures 152
- **educational history** 90
- **elected officials**
  - constituency records 11
  - correspondence 11
  - disclosing personal information to 228
  - meetings 131
  - personal records 11
- **elections**
  - local public bodies 11
- electronic forms, *see* **forms**, electronic
- electronic mail, *see* **records**
- electronic records, *see also* **records**
  - audit trails 257

  correcting 205
  creating new records from 59
  defined 254
  destruction 258
  disposition 258
  documentation 251
  management 256–59
  matching 240
  retrieval 47
embarrassment 67
emergencies
  collecting personal information 193, 199
  contact persons 193
  disclosing personal
    information 84, 218, 231
emergency planning 108
emissions
  toxic 181
employees
  as confidential sources 110, 159
  disclosing personal information
    to 223–25
  disclosure to the Information and
    Privacy Commissioner 184–85, 291
  emergency contacts 194
  grievances 107
  identities 184, 291
  personal information
    disclosure 84–85, 217, 233
  research information 147, 149
  theft 106
employment
  administrative investigations 107
  adverse actions 29, 185
  confidential evaluations 101–4
  contracts 85, 217
  discretionary benefits 85, 217
  duties 90
  interviews 103
  job classifications 84, 139, 217, 228
  job counselling 227
  job responsibilities 84, 217
  leaves of absence 85
  pay and benefit services 198
  peer evaluations 103
  performance appraisals 90, 91, 103, 139
  personal information 5, 90
  personal service contracts 85, 139, 217
  references 91, 102, 198, 221
  selection process 102, 139
  staffing requirements 139
employment history 90, 115
employment information, *see* **employees**,
  personal information; **personnel
  information**
employment insurance 222, 227
enactments of Alberta
  collecting personal information 190
  disclosing personal
    information 84, 221–23
  disclosing third party information 79
  routine disclosure 16
enactments of Canada
  collecting personal information 190
  disclosing personal
    information 84, 221–23
  disclosing third party information 79
  routine disclosure 16
endangered forms of life
  disclosure harmful to 164–65
ENMAX Corporation 3
enrolment information
  post-secondary educational
    bodies 87, 218
  schools 87, 218
environment
  disclosure to protect
    fee waiver 55
    personal information 92–93
  harm to 181
  testing 142, 149–50, 152
Environmental Appeal Board 8
EPCOR Utilities Inc 3
espionage 109
estates
  administration of 197, 246
Ethics Commissioner
  disclosing personal information to 234
  office 2
  records 9
  records excluded from *FOIP Act* 8
ethnic origin 91
  personal information 5
evaluations
  confidential 101–4
examination for discovery 4
examination of records, *see* **records,**
  examination of
examination questions 9
exceptions, *see* ***FOIP Act***, exceptions
exclusions, *see* ***FOIP Act***, exclusions

Executive Council 2
  agenda 125
  appeals 127
  background facts 127–28
  Cabinet confidences 124
  confidential information 124–29
  decisions 127–28, 160
  defined 125
  members, *see* **ministers**
  minutes 125
  non-arm's length transactions 13
executors 246
exhibitions 219
existence of records 63
  failure to locate 63
  harm to health or safety 65, 99–100
  harm to law enforcement 65, 117
  personal information 65, 95–96
experts
  disclosing personal information
    to 99, 232, 366–67, 368

F

factual information
  not advice 137
fair information practices 187–89, 261–86
fair trials 112
family relationships 94, 235–36
family status 5
family violence 98
fauna
  conserving 164
Federal Bureau of Investigation 231
federal government, *see* **Government of Canada**
federation boards, *see* **library boards**
fees
  assessing 50–52
  collecting 24, 63
  continuing FOIP requests 51
  deposits 54
  estimates 52–54, 333–34
  examination of records 51
  FOIP requests 24
  GST 51
  initial fees 51
  investigations 301
  licensing databases 20
  local public bodies 51
  outstanding 63
  payments 54
  personal information requests 50, 52
  reducing 55
  refunds 46, 53, 54
  routine disclosure 17
  schedule 51
  waivers 51, 54–56
field trips
  lists of participants 219
Financial Administration Act 12
financial audits 227–28
financial gain 77
financial history
  personal information 5
financial information 74, 85, 86, 147–48, 217
  public bodies 146
financial loss 77, 148
fines
  collection of personal information 195
  disclosure to collect 225–26
  offences under the *FOIP Act* 30, 185
fingerprints 5
fire commissioners 230
fire inspections 116
fire investigations 106
firearms
  permits 113
  technical information 113
First Nations police services 4, 230
fishing licences 86
flora
  conserving 164
FOIP Act
  adjudicator process 302–3
  administration 23–30
  advice 290–91
  amending 27
  annual report 27, 289
  burden of proof 299–300
  contracts and contractors 7
  exceptions 1, 67–166
    advice from officials 134–44
    Cabinet and Treasury Board confidences 124
    confidential evaluations 101–4
    exposure to civil liability 114–15
    harm to business interests 73–81, 244
    harm to economic and other interests of public bodies 145–51

    - harm to historic resources 164–65
    - harm to individual or public safety 98–101
    - harm to intergovernmental relations.............................. 119–23
    - harm to law enforcement.. 105–18, 244
    - harm to personal privacy 82–96
    - individual under supervision of correctional authority 114–15
    - interpretation 67
    - local public body confidences .. 130–34
    - notices 339–41
    - offence under Act of Canada.......... 115
    - privileged information...... 153–63, 244
      - third parties 156–57, 161
    - published information 165–66
    - relevant factors 67
    - steps in applying.............................. 80
  - exclusions 1, 7–14
    - disclosure...................................... 14, 60
    - notices 339–41
  - exercise of rights by other persons....................................... 246–48
  - monitoring 289–90
  - offences and penalties..... 29–30, 185, 210
    - destruction of records 252
  - policies and procedures 24
  - province-wide administration 27–29
  - public education................................... 288
  - purposes 1, 56, 67, 71
  - relationship to other Acts............... 14, 24, 72, 87
    - archival records 242
  - scope 1–3, 4–5
  - steps in applying 71
  - time extensions
    - third parties............................... 174–75
  - training.. 24, 28
- ***FOIP Bulletins***
  - Number 1, Fee Estimates...................... 53
  - Number 2, Fee Waivers 56
  - Number 3, Manuals and Reading Rooms 33
  - Number 4, Disclosure of Personal Information – Section 16(2)(j) 218
  - Number 5, Fund-Raising 214
  - Number 6, Records of Elected and Appointed Officials of Local Public Bodies 11, 12
  - Number 7, Law Enforcement 105
  - Number 8, Common Programs and Services 225
- FOIP contacts, *see* **programs and services**, FOIP contacts
- **FOIP Coordinator**
  - closure of office 45
  - collection of personal information 191
  - consultations
    - Cabinet and Treasury Board confidences................................ 125
    - intergovernmental relations 122
  - copies of requests and records 65
  - creating new records 59
  - delegation orders 27
  - duty to assist 24, 34, 59
  - FOIP requests...................... 24, 38, 49, 65
  - information dissemination 19
  - privacy audits......................... 24, 371–77
  - privacy impact assessments 263
  - privacy protection 188
  - records management 25
  - relationship with applicants 34, 37
  - responsibilites 23–24, 46
  - review of records 48, 58
  - routine disclosure............................ 17, 24
  - severing information 24
- ***FOIP: Guide to Developing Personal Information Sharing Agreements*** 222
- FOIP Office, *see* **FOIP Coordinator**
- **FOIP Regulation**
  - amending.. 27
  - audits.. 227
  - consent for use of personal information 212
  - consent to disclosing personal information 220
  - fee schedule 51
  - harm to applicant's health and safety 99, 232
  - *in camera* meetings 131
  - public bodies... 24
    - agenda or minutes............................ 140
  - relationship of *FOIP Act* to other Acts . 72
  - research agreements.................... 241, 244
  - responding to a request 64
  - using personal information 212
- **FOIP requests**
  - abandoning.............................. 56, 335–36
  - access 63
  - acknowledging 35, 326
  - adequacy of search........................ 250–53

  as last resort ... 15
  clarifying ... 37
  communications strategies ... 25
  concurrent ... 44
  consultations ... 40, 41, 42, 49
    third parties ... 167–76
  continuing, *see* **continuing FOIP requests**
  copying records ... 48
  deemed refusal ... 42
  disregarding ... 36, 292–94
  documenting ... 38, 44, 58, 62, 296, 391
  evading ... 29
  exercising discretion ... 69, 70–72
    reconsidering ... 70
  fees, *see* **fees**
  forms ... 34, 391
  frivolous or vexatious ... 37, 293
  in camera meetings ... 132
  Information Management and Privacy role ... 40
  initial fees ... 51
  language ... 34
  legal advice ... 58
  legal case records ... 4
  line-by-line review ... 49, 57–59, 61, 71, 391
  multiple ... 44
  narrowing ... 35, 37, 38, 53
  nature of ... 33
  notices ... 41, 49–50, 57 167–72, 325–68
  oral requests ... 34
  partial disclosure ... 49, 63
  personal information ... 216
  preliminary assessment ... 48–49
  preliminary examination of records ... 71
  processing ... 24, 25, 46–65
  prosecutions ... 116
  receiving ... 33–46, 326
  records excluded from *FOIP Act* ... 14, 64
    refusal of access ... 63
  records issues ... 250–53
  records retention ... 65
  refusal of access ... 61, 62, 64, 339–41, 342, 343
  refusal to confirm or deny existence of records ... 63, 65, 95–96, 99, 117, 343
  repetitious ... 36, 292
  responding to ... 45, 61, 62–65, 72, 296
    notices ... 337–43
  responsive information ... 59–60
  review for routine disclosure ... 19
  reviewer's recommendations ... 58
  scope ... 35, 38
  severing ... 59–62, 67, 71
    documenting ... 68
    non-responsive information ... 60
  statistics ... 28
  systematic ... 36, 292
  time extensions ... 38, 331–32
  time limits ... 38, 41–46, 49, 172–74
  tracking ... 24, 28, 35, 38, 39, 46, 49
  transfers ... 39–41, 45, 49
    notices ... 330

FOIP requests
  documenting ... 391
  forms ... 391

forms
  collection of personal information ... 189, 199
  electronic ... 276
  FOIP requests ... 34
  review ... 274–77

foundations, *see* **housing management bodies**

Freedom of Information and Protection of Privacy: Contract Manager's Guide ... 7, 189, 259, 280

Freedom of Information and Protection of Privacy Act, *see* ***FOIP Act***

Freedom of Information and Protection of Privacy Regulation, *see* **FOIP Regulation**

frivolous or vexatious FOIP requests ... 36-37, 292-93

fund-raising
  alumni records ... 214, 236
  collecting personal information ... 194
  disclosing personal information ... 236
  events
    attendance ... 219

G

gangs ... 111
genealogical research ... 86
general faculties councils ... 12, 131
General Revenue Fund ... 54
Glenbow-Alberta Institute
  archives ... 229
good faith ... 184

- goods and services tax, *see* **GST**
- **good will** 77, 148
- **governing bodies**
  - advice and deliberations 135
  - agenda or minutes 140
  - appointees 84
  - correspondence 12
  - designation of head of public body 23
  - meetings 131
  - personal records 12
  - post-secondary educational bodies 12, 131
  - roles and responsibilities 23
- **Government of Alberta** 1
  - as sovereign power 119, 146
  - economic interests 145–51
  - intergovernmental relations 119–23
  - investment strategies 146
  - negotiations 138–39
  - non-arm's length transactions 79
  - personnel management 198, 233
- **Government of Canada** 108–9
  - intergovernmental relations 119
- ***Government Organization Act*** 203, 210
- **graduations**
  - certificates or awards 219
  - lists of graduates 218, 219
- **grants** 86
  - eligibility for 227
- **grievances** 107
- **GST** 51
- **guardians** 95, 197
  - exercising rights of individuals 247
  - exercising rights of minors 247–48
- ***Guide to Identifying and Disposing of Transitory Records*** 256

H

- **harassment** 98
  - administrative investigations 107
- **harm**
  - atmosphere 181
  - audit procedures 152
  - business interests 73–81
  - currency of 69
  - determining 57, 69, 76
  - economic interests of public bodies 145–46
  - environment 181
  - exposure to 87, 94
  - financial gain 77
  - financial loss 77
  - health or safety 181
  - historic resources 164–65
  - intergovernmental relations 119
  - law enforcement 108, 109
  - monetary value 76
  - privacy 82–96
  - probability of 69, 76
  - public interest 76, 77, 179
  - specifying 69
  - testing procedures 152
- **harms tests** 69, 76, 145–46
- **heads of public bodies**
  - administrative investigations 107
  - advice and deliberations 135
  - advice from Information and Privacy Commissioner 288
  - disclosing personal information to 224
  - disclosure harmful to intergovernmental relations 121
  - discretionary exceptions reconsidering 70
  - disregarding FOIP requests 292–94
  - exercising discretion 70
  - requiring Informaton and Privacy Commissioner to examine records 292, 298
  - responsibilities 23
- **health** 5
  - disclosure endangering 83–84, 361
  - disclosure harmful to 87, 98–101, 218
    - refusal to confirm or deny existence of records 65
  - harm to 181
  - imminent danger to 236
  - legislation
    - relationship to *FOIP Act* 72, 87
- Health and Wellness, Department of, *see* **Alberta Health and Wellness**
- **health care**
  - personal information 5, 87, 90, 115, 218, 222
    - expert consultations 98, 99, 232
  - research 149
- **health care bodies** 2
  - disclosing personal information 87
  - patient information 87
- **Health Facilities Review Committee** 106
- **hearing-impaired persons**
  - FOIP requests 34

- **historic resources**
  - disclosure harmful to 164–65
  - impact assessments 164
- **historic sites** 164
- historical research, *see* **research,** historical
- ***Historical Resources Act***
  - section 1(f) 164
- **holidays** 45
- **honours**
  - receipt of 88, 219
  - suitability for 194
- **hospital boards** 2
- **Hospital Privileges Appeal Boards** 112
- **hospitals**
  - admission 87, 115, 218
- ***Hospitals Act*** 2
- **housing**
  - low-income 102, 196
    - continuing eligibility for 197
  - student 102
- **housing authorities** 3
- **housing management bodies** 3, 12
  - audits 228
- human resources, *see* **employment**; personnel management
- Human Resources and Employment, Department of, *see* **Alberta Human Resources and Employment**
- **Human Resources Development Canada** 222
- ***Human Resources Guide for Local Public Bodies*** 233
- **human rights panels** 112
- **hunting licences** 86

I

- **identifiers**
  - removal 241
- ***Identifying Personal Information Banks: A Guide for Local Public Bodies*** 32
- ***Identifying Personal Information Banks: A Guide for Provincial Government Ministries*** 32
- **identity**
  - applicants 17, 46, 168, 170
  - confidential sources 110
  - employees 184, 291
  - police informers 110
  - proof of 17, 63
  - third parties 170
- **implementation**
  - public body plans 139
- **improvement districts** 2
- ***in camera* meetings**
  - local public bodies 131–32
  - minutes 132
  - municipalities 131
  - personal notes 132
- **income assistance** 86, 90, 196, 201, 221
  - Alberta Seniors Benefit 196, 222
- **incompetent individuals** 213, 296
- ***Indian Act* (Canada)** 120
- indirect collection, *see* **personal information**, indirect collection; **collection of personal information**, indirect
- **industrial sabotage** 109, 111
- **information**
  - 5 years old
    - Cabinet decisions 128
  - 15 years old
    - advice from officials 141
    - Executive Council or Treasury Board 126
    - intergovernmental relations 122
    - local public body confidences 133
  - 25 years old
    - disclosure by archives 244
  - 50 years old
    - businesses 80
  - available for purchase 165
  - correctional records 114
  - disclosure in public interest 178–85
  - disclosure policies 70
  - failure to publish 166
  - individually identifiable 5–6, 239
  - law enforcement records 114
  - leaks 127
  - local public body confidences 130–34
  - published 74, 165–66, 234–35
    - fund-raising 194
  - revealing classes of 69
    - advice from officials 134–44
    - criminal intelligence 110
  - third party legal 161
- **Information and Privacy Commissioner** 287–303
  - adjudicator process 302–3
  - advice 290–91
    - defined 137
  - advice to heads of public bodies 288

annual report 28, 289
appeals
  fees 55
appointment 287
approval of research purposes 239
as public body 2, 287, 302–3
audits 24, 290, 371–77
burden of proof 299–300
comments
  proposed legislation 288
  proposed programs 288
complaints, *see* **complaints**
conflict of interest 287, 302–3
contempt of court 291, 298
data matching 284
decisions 68
delegation by 295
disclosure of information by 294
disclosure of third party information 172
disclosure to 184–85, 234, 291
disclosure to Minister of Justice and Attorney General 294
discretionary exceptions
  orders 70
disregarding FOIP requests 36, 292–94
duty to assist applicants
  comments 288
evidence in proceedings 294
examination of records 292, 298
excluded records 63
forms 391
indirect collection of personal information 192
inquiries 298
  refusal to conduct 299
investigation reports 301
investigations 24, 288, 295–302, 301
  disclosure by employees 184, 291
  duty to assist 301
  failure to disclose in public
    interest 184
  fees 301
  personal information correction 301
  records management 250
  time extensions 301
judicial review 303
mediation 297–98
monitoring *FOIP Act* 289–90
notices
  substitutional service 168
notification of disclosure in public interest 183–84
obstruction 29
offences 29
  laying charges 294
office 2
orders 288, 289
  administrative matters 288
  compliance 300
    offences 29, 300
  discretionary exceptions 70, 300
  judicial review 289, 303
  mandatory exceptions 300
  personal information 288
  precedents 71
  time limits 300
  types 300–301
parliamentary privilege 159
personal information requests 36
powers 287–89
  delegation 295
  inquiries 298
  investigations 291
practice notes, see ***IPC Practice Notes***
privacy audits 302
privacy impact assessments 262, 263
privacy protection 289–90
privileged information 294
producing records for 291–92
  time limits 298
protection from liability 294–95
public education role 288
public interest
  determination 182
  fee waivers 56
records excluded from *FOIP Act* 8, 14, 64
record linkage
  comments 288
records management 250
refusal to confirm or deny existence of records 63
refusing access 63
removal from office 287
requesting a review 63
research 288
responsibilities 28, 287–91
  records management 250
retention of records reviewed 298
review process 297

reviews, *see* **reviews**
severing information 297
statements provided to 294
term of office 287
third party consultations 168
time extensions 42, 43
third party notification 172
information dissemination 16–18
information management ... 25–26, 249–59
policy and procedures 254–59
principles 253–54
Information Management and Privacy
adjudication and adjudicators 303
FOIP home page 38
FOIP request coordination 40
personal information
new use of
disclosure 273–74
publications 7, 11, 12, 28, 32, 33, 53, 56, 105, 189, 214, 218, 222, 225, 233, 259, 280
relationship of other Acts to *FOIP Act* . 72
responsibilities 28
tracking system 39
training 28
information technology and systems
active dissemination 19
planning 254, 257
policies and procedures 254
privacy protection 257, 261–86
records management 256–59
security 106, 209, 278–79
infrastructure
provincial 146
inheritable characteristics 5
law enforcement 109
inheritance rights 93
inmates
legal representatives 236
Innovation and Science, Department of, *see* **Alberta Innovation and Science**
inquiries, *see* **Information and Privacy Commissioner**, inquiries
inspections
fire 116
liquor licensing 116
practices 146
public health 116
reports 75, 116
routine
law enforcement 116
routine disclosure 19
integrated programs or services, *see* **programs and services**, integrated
intelligence tests 152
intergovernmental relations
negotiations 119–23
records
15 years old 122
refusing to disclose information ... 119–23
International and Intergovernmental Relations, Department of, *see* **Alberta International and Intergovernmental Relations**
international bodies
intergovernmental relations 119
International Labour Organization 120
Internet
active dissemination 16, 20
collecting personal information
from 194
disclosing personal information on 235
FOIP home page 38
routine access 16
Interpol 231
Interpretation Act 45
interviews 103
collection of personal
information 189, 199
notes
retention 202
investigations
administrative 106
authority for 106
Attendance Boards 106
by-law 106
collection of personal information 195
complaints as part of 105
corporate security 106
disclosure of personal information
for 90, 230–31
fire 106
Information and Privacy Commissioner, *see* **Information and Privacy Commissioner**, investigations
investigative techniques 109
law enforcement 105–7
disclosure form 391
interference with 111
police 106
completed 116
Safety Codes Act 106

  security 106, 280
investment strategies 74, 148
  public bodies 146
IPC Practice Notes
  1, Applying "harms" tests 69
  2, Informing the applicant of grounds for refusal 62, 297
  3, Complaints about public bodies – "Reviews" versus "Investigations" 301
  4, Section 4 – Exclusions from the *Act* 14, 292
  5, Preparing records and submissions for inquiries 297
  7, Privacy complaints – investigations and inquiries 301
Irrigation Act 3

J

jobs, *see* **employment**
judges
  records 7
judicial administration records 7
judicial review 289, 303
judicial tribunals
  disclosure of personal information to 232–33
  draft decisions 7
  rules 4
Justice and Attorney General, Department of, *see* **Alberta Justice**
justices of the peace
  records 7

L

labour relations
  disputes 78
  in camera meetings 132
  information 74, 77–78
  mediation 78
  negotiations 138–39
  officers 78
  third parties 77
Labour Relations Board 78
labour unions
  archival records 10
  associations 5, 91
  collective agreements 74
  disclosing personal information to 229
  membership 91
land claims 94, 120, 199
Land Titles Offices 10
landfills
  testing 142
law enforcement
  agencies 230, 231
  collection of personal information 190, 195
  complaints 108
  confidential sources 110
  criminal intelligence 110–11
  disclosure harmful to 105–18
  disclosure of personal information
    for 230–31
    forms 391
  DNA testing 109
  harm 108
  in camera meetings 132
  inspections 116
  investigations 105–7
    interference with 111
  investigative techniques 109
  legal proceedings 107
  penalties or sanctions 105
  privileged information 158
  records
    custody or control 105
    disclosure 105–18
    disclosure an offence under Act of Canada 115
    personal information 90
    severing information 62
  records of disclosure 230
  refusal to confirm or deny existence of records 65, 117
  reports and publications 116
  routine inspections 116
  statistical information 116
  unsolved investigations
    interference with 111
Law Enforcement Disclosure Form 391
law reports 235
lawsuits 4
leaks of information 127
Learning, Department of, *see* **Alberta Learning**
leases 77
  Crown land 86
legal agents 161

legal matters
- advice, 154, 155
  - compliance with subpoena, warrant or order, 223
- applicant's rights, 93
- civil legal cases, 4, 114, 225
- collection of personal information, 196
- correspondence, 161
- criminal legal cases, 4
- disclosure of personal information, 225
- fair trial, 112
- FOIP advice, 58
- impartial adjudication, 112
- *in camera* meetings, 132
- legal actions, 112
- legal instruments, 131

legal opinions, 155

legal privilege, 154–62
- severing, 60

legal proceedings, 112
- access to records, 4, 10
- collection of personal information, 196
- disclosure of personal information, 225, 232–33
- law enforcement, 107

legal representatives
- inmates, 236

legislation
- drafts, 139–40
  - Executive Council, 126
  - Information and Privacy Commissioner comments, 288
- interpretation, 143

Legislative Assembly, 287

Legislative Assembly Act, 222, 224

Legislative Assembly Office, 2, 12

letters, 5
- elected officials, 11
- governing bodies, 12

liabilities
- financial
  - public bodies, 146

liability
- civil
  - discretionary exceptions, 114
- protection from, 29, 185, 294–95
- public bodies, 67

libraries
- active dissemination, 20, 166
- head, 23
- information dissemination, 18
- membership, 227
- school-housed, 225

Libraries Act, 3

library boards, 3, 12

library system board, *see* **library boards**

licences
- drivers, 10
- personal information
  - disclosure, 85–86, 217
- suspension or revocation, 86
- trade secrets, 74, 147

licensing
- databases, 20
- practices, 146

Lieutenant Governor in Council
- draft judicial or quasi-judicial decisions, 7

literacy
- FOIP requests, 34
- programs
  - collection of personal information, 201

litigation privilege, 156–57

local government bodies, 2
- confidential information, 119–23
- intergovernmental relations, 119–23, 119

local public bodies, 2–3
- by-laws, 5, 130, 131
- databases, 18
- directories of records, 32
- elected officials, 11–12
- elections, 11
- fee structures, 51
- heads, 23
- *in camera* meetings, 130–34
  - authority for, 131–32
- meetings, 131
- personal information
  - disposition, 210
- personal information banks, 32, 255
- personnel management, 233
- records management, 5, 249–59
  - FOIP requests, 65
- security, 106
- transitory records, 256

long-term care facilities, *see* **nursing homes**

M

maintenance enforcement
  collection of personal information 197
  disclosure of personal information 233
Maintenance Enforcement Act 233, 242
management bodies, *see* **housing management bodies**
mandatory exceptions 68
  Cabinet and Treasury Board confidences 124–29
  creating new records 20
  harm to business interests 73–81, 244
    steps in applying 80
  harm to personal privacy 82–96
  notices 339–41
  offence under Act of Canada 115
  privileged information
    third parties 161
  public interest 68
  tax information 78–79, 91
manuals and guidelines
  accessing 32–33, 143
mapping data
  proprietary interest 148
maps 5, 165
marital status 5
markets
  regulating 146
media
  specialized 60
mediation
  Information and Privacy Commissioner 297–98
  labour relations 78
medical records 8, 160
meetings
  local public bodies 131
Members of Parliament 228
Members of the Legislative Assembly (MLAs)
  correspondence 12
  disclosing personal information to 228
  offices 3, 12
  records excluded from *FOIP Act* 3, 12
mental disabilities 5
mental health, *see* **health**
metis settlements 3
Metis Settlements Act 3
Metis Settlements General Council 3
Metropolitan Police 231
Minister of Justice and Attorney General 233
  as legal agent 161
  correspondence 161
  disclosure to by Commissioner 294
  prosecutions 112
Minister responsible for the *FOIP Act*
  adjudicator's expenses 303
  annual report 27
  copies of orders 300
  FOIP Coordinator 24
  intergovernmental relations 121
  responsibilities 27–29
ministers
  advice and recommendations 137–38
  advice to 134–44
  constituency records 3, 12
  consultations or deliberations 138
  correspondence 12, 125
  disclosing personal information to 223–24
  heads 23
  non-arm's length transactions 13
  offices 2
  orders, drafts of 139–40
  personal records 3, 12
  records 10
  statements 127
minors 31
  disclosure of personal information 247–48
minutes
  consultations or deliberations 138
  Executive Council 125
  in camera meetings 132
  public bodies 140
Model Code for the Protection of Personal Information 187
monetary value
  economic interests of public bodies 148
Motor Vehicle Accident Claims Act 236
Motor Vehicle Registry 10
Municipal Affairs, Department of, *see* **Alberta Municipal Affairs**
municipal councillors 11
Municipal Government Act 2, 78
  in camera meetings 132
  part 15.1 2
  sections 299–301 72

municipal library boards, *see* **library boards**

municipalities 2
- by-laws 90, 130
- closure of office 45
- head 23
- historic resources 164
- *in camera* meetings 131
- police commissions 3
- policing committees 3
- tax information 78
- twinning 120

N

names
- personal information 5
- unreasonable invasion of privacy 91

national origin
- personal information 5

national security 108–9

native people, *see* **aboriginal people**

natural gas leaks 181

negotiations
- aboriginal people 120
- contractual 138–39, 149
- disclosing information 138–39
- economic interests 146
- intergovernmental relations 119, 122
- positions 76
- public bodies 149
- third parties 76, 149

next of kin 193

non-arm's length transactions 13, 79

Northern Alberta Development Council 13

notes
- handwritten 5
- interviews 202
- personal, *see* **personal notes**
- transitory records 256

notices
- applicants 170, 326–43
- collection of personal information 199–201, 267–69, 274–77
  - exceptions 200
  - verbal 199, 275
- continuing FOIP requests 329
- correction of personal information 207–8, 362–65
- data matching 273, 281–86
- disclosure of personal information 84, 225
- disclosure to experts 366–67, 368
- fee estimates 53, 333–34
- FOIP requests 49–50, 325–68
  - abandoning 57, 335–36
  - transfers 41, 330
- parliamentary privilege 344
- public interest disclosure 359, 360
- public interest disclosure 183–84
- refusal to confirm or deny existence of records 343
- representatives 248
- service of 168
  - substitutional service 168
- third parties 45, 167–72, 345–61
  - content 169–70
  - correction of personal information 207–8
- time extensions 45, 331–32

notification, *see* **notices**

numbers or symbols
- personal information 5

nursing homes 2
- admission to 227
- residents 87, 218

Nursing Homes Act 2

nursing programs 225

O

OECD Privacy Guidelines 187

offences 29–30
- Acts of Canada 115
- adverse employment action 185
- destruction of records 29, 48, 210, 252
- *FOIP Act* 29, 185
- investigation 105
- non-compliance with Information and Privacy Commissioner's orders 300
- parking 106

Office of the Information and Privacy Commissioner, *see* **Information and Privacy Commissioner**

officers
- public bodies
  - disclosing personal information to 223–25

- **Officers of the Legislature**
  - administrative files 9
  - disclosure of personal information to 234
  - records excluded from *FOIP Act* 8
- **offices** 1
  - agenda or minutes 140
  - public bodies
    - closure 45
- ***Official Secrets Act* (Canada)** 115
- **Ombudsman** 289
  - disclosing personal informaion to 234
  - office 2
  - records excluded from *FOIP Act* 8
- ***Ombudsman Act***
  - section 24(3) 159
- **Ontario Information and Privacy Commissioner**
  - Order M-850 37
- **open houses**
  - attendance 219
- **opinions**
  - correction of 204, 206
  - personal information 5
- **oral requests** 34
- **orders**
  - disclosing personal information 223
- **Organization for Economic Cooperation and Development** 187

P

- **palaeontological resources** 164
- **papers** 5
- paramountcy, *see* ***FOIP Act***, relationship to other Acts
- **parking offences** 106
- **parliamentary privilege** 159
  - notices 344
- **parole** 113, 114, 115, 196
- **partnerships** 167
- **pastoral care**
  - disclosing personal information 218
- **patients** 87
- **payments**
  - disclosure to make 225–26
- **peace officers** 113
- **peer evaluations** 103
- **penalties**
  - *FOIP Act* 29–30, 185, 252
- **penalties or sanctions**
  - breach of security 280
  - law enforcement 105
- **permits**
  - firearms 113
  - personal information disclosure 85–86
  - property 85–86, 217
  - suspension or revocation 86
- ***Personal Directives Act*** 247
- **personal information**
  - access 1, 36, 67
    - audits 373
  - accuracy 201–3, 269–70
    - audits 373
    - delegation of authority 27
    - every reasonable effort to ensure 202
  - agreements authorizing disclosure
    - contents of 222
  - annotation 205–7
    - forms 391
  - awards 88, 219
  - collection 189–201, 267–69
    - agreements between public bodies 189
    - audits 371–73
    - collecting fines or debts 195
    - contracts and contractors 189, 190
    - correctional authorities or institutions 195
    - direct 192, 267–69
    - emergencies 193
    - forms 199, 274–77
    - from Internet 194
    - from other public bodies 193
    - fund-raising 194
    - honours or awards 194
    - indirect 192–99
    - interviews 189, 199
    - investigations 195, 301
    - law enforcement 190, 195
    - legal matters 196
    - legal proceedings 196
    - limitations on 190
    - literacy programs 201
    - maintenance enforcement 197
    - means of collecting 189
    - methods 192–201, 267–69
    - notices 199–201, 267–69, 274–77
      - exceptions 200
    - personnel management 198
    - programs and services 190

  - provision of legal services 196
  - purposes 189–92, 212, 237
  - registries 11
  - review of practices 191
  - unauthorized 209
- compiling 219
- confidential 94, 99
- consent to disclosure 83
  - bargaining agents 229
  - exercise by other persons 83
  - MLAs 228
  - procedures 220
- consent to new uses
  - procedures 212
- consistent use 219, 237–38
  - audits 375
- constraints on disclosure 215, 225
  - law enforcement 231
- constraints on use 214, 237, 264
- correction 1, 40, 203–8
  - audits 373
  - delegation of authority 27
  - investigations 301
  - notices 207–8, 362–65
  - opinions 204, 206
  - time limits 205, 207
- data matching 240, 265, 273, 281–86, 375
- data sharing 273, 281–86
- deceased individuals 86, 217, 235–36, 243, 246
- defined 5–6
- direct collection 192, 199, 200
- disclosure 82–96, 215–37, 238–48, 272
  - archival purposes 229–30, 242–45
  - audits 227–28, 374–75
  - collecting fines or debts 225–26
  - common programs and services 224–25
  - compliance with enactments 221–23
  - compliance with subpoena, warrant or order 223
  - consent 83, 220, 228, 229
  - consistent use 219
  - constraints on 215, 225, 240
  - correctional authorities or institutions 233, 234
  - court proceedings 232–33
  - deceased individuals 235–36, 246
  - delegation of authority 27
  - discretionary benefits 85–86, 217
  - emergencies 84, 231
  - employee information 84–85
  - enforcing legal rights 225
  - expert consultations .. 232, 366–67, 368
  - for investigations 90, 230–31
    - forms 391
  - for purposes of collection 193, 219
  - guardians 247–48
  - health or safety danger 83–84
    - notices 361
  - Internet 235
  - investigations 301
  - judicial tribunals 232–33
  - labour unions 229
  - law enforcement 230–31
  - legal matters 225
  - legal proceedings 225, 232–33
  - licences and permits 85–86, 217
  - maintenance enforcement 233
  - making payments 225–26
  - minors 247–48
  - not contrary to public interest 86–89, 217
  - not unreasonable invasion of privacy 82–89, 167, 217–19, 243
  - notices 84, 225
  - Officers of the Legislature 234
  - pastoral care 218
  - personnel management 233
  - proof of identity 17, 63
  - protection of environment 92–93
  - public events 88
  - public health 92–93
  - public information 234–35
  - public interest 92–93, 216
    - limitations 180
  - public safety 92–93
  - public scrutiny 92–93
  - quasi-judicial proceedings 232–33
  - quasi-judicial tribunals 232–33
  - record of purposes 246, 273–74
  - records of 216
  - refusal of consent 220
  - research purposes 84, 232, 238–45, 272–73, 376
  - restrictions on archives 244
  - statistical purposes 84, 232, 238–45, 272–73, 376
  - to avert imminent danger to health or safety 236
  - to bargaining agents 229

    - to employees 223–25
    - to ministers 223–25
    - to MLAs 228
    - to Ombudsman 234
    - to representatives 246–48
    - unauthorized 210, 216
    - unreasonable invasion of privacy 36, 89–96, 247–48
      - determining 91–95
    - use after 213–14
    - vehicle accidents 236
    - verifying eligibility 226–27
  - discretionary benefits 85–86
  - disposition 210–11
  - errors 204
  - honours 88, 219
  - identifying
    - for disclosure 220
    - new uses 212
  - inaccurate 95, 200
  - inadvertent disclosure 89
  - *in camera* meetings 132
  - indirect collection 192–99
    - authorized by Information and Privacy Commissioner 192
    - authorized by enactments 192
    - authorized by individual 192
  - individually identifiable 5–6, 239–40
    - removal of identifiers 241
  - law enforcement records 90
  - less than 25 years old 243
  - licences 85–86
  - limitations on access 67
  - linkage 205–7, 240, 265, 288
  - minors 247–48
  - notices to experts 366–67, 368
  - offences 29
  - omissions 204
  - opinions 5, 204, 206
  - permits 85–86
  - police officers 113
  - protection 208–11, 270–71
    - audits 373–74
    - physical security 209
  - public interest
    - limited disclosure 180
  - records excluded from *FOIP Act* 187
  - records more than 75 years old 244
  - refusal to confirm or deny existence of records 95–96
  - refusal to disclose individual's own 98, 101–4
  - registries 10
  - request for non-disclosure 88–89, 217
  - research agreements
    - contents of 240–42, 391
  - retention 201–3, 269–70, 376–77
  - routine disclosure 4, 17–18, 216
  - sharing by public bodies 193, 265, 278
  - supplied by applicant 95
  - suppressing 20
  - taxes 91
  - third parties 15, 94
    - consultations 167–76
  - unauthorized access 209
  - unauthorized destruction 210–11
  - unreliable 95
  - updating 202
  - use 211–14, 272
    - audits 374
    - consent to new uses 212
    - constraints on 214, 237, 264
    - disclosed by other public bodies 213–14
    - fund-raising 214
    - investigations 301
    - record of purposes 273–74
    - unauthorized 210
  - verification of 202
  - verifying eligibility for programs or services 196–97
- **Personal Information Annotation Form** 391
- **personal information banks** 24, 26, 28
  - contents 31
  - directories 31, 255
  - local public bodies 32, 255
  - management 376
  - provincial public bodies 31–32, 273–74
  - purposes 216, 246
  - record inventories 255
- ***Personal Information Protection and Electronic Documents Act* (Canada)** 187
- **personal information requests** 36, 216, 217
  - correction 204–7
    - disregarding 292–94
    - forms 391
    - notices 362–65

    - refusal 205–7
    - transfers 39–41, 208
  - defined 36
  - fees 50, 52
  - forms 391
  - policies and procedures 373
  - refusal of access 61, 62
  - refusal to disclose applicant's
    - information 98, 101–4
  - representatives 36, 246–48, 391
  - responsive information 60
  - transfers
    - correction of information 39, 208
- **personal information systems** 261–86
  - audits 371–77
  - contracting out 266
  - reviews 266–74
- **personal notes** 7
  - elected officials 11
  - *in camera* meetings 132
- personal opinions, *see* **opinions**
- **Personal Property Registry** 10
- personal records, *see* **elected officials**, personal records; **governing bodies**, personal records; **ministers**, personal records
- **personal service contracts** 85, 139, 198, 217
- **Personnel Administration Office** 198, 233
- **personnel information**
  - disclosure
    - not unreasonable invasion of privacy 84–85, 217
    - unreasonable invasion of privacy 90, 91
- **personnel management**
  - administrative investigations 107
  - audits 152, 228
  - collection of personal information 198
  - disclosure of personal information 233
  - grievances 107
  - local public bodies 233
  - plans 139
  - security 279
  - third parties 74
- **personnel records**
  - routine disclosure 17–18
- persons with disabilities, *see* **disabled persons**
- **photographs** 5
  - honours and awards 88
  - public events 88
  - sporting events 219
  - students 87
- physical health, *see* **health**
- **physicians**
  - expert consultations 98, 99, 232
- **plans**
  - technical 74
- ***Police Act*** 3, 106
- **police and policing**
  - criminal intelligence 110–11
  - defined 105
  - informers 110
  - investigations 106
    - completed 116
  - peace officers 113
  - police officers
    - personal information 113
  - special constables 102, 106, 113
- **police commissions** 3
- **police services** 3, 230, 231
  - prosecutions 112
- **policies and procedures**
  - advice and recommendations 137–38
  - archival records 245
  - compliance with *FOIP Act* 24
  - disclosure of course evaluations 237
  - disclosure of information 70
  - disclosure of personal information 216, 217
  - disclosure to MLAs 228
  - information management 254–59
  - information technology and systems 254
  - instructions or guidelines 143
  - interpretation 143
  - pending policy decisions 140
  - personal information requests 373
  - personal information systems 266–74, 377
  - records management 254–59
  - security 208
- **policing committees** 3
- **policy advice**
  - background materials 142
  - confidentiality 138
  - Executive Council or Treasury Board 126
  - officials 134–44

- ***Policy for Maintaining Security of Government Data Stored on Electronic Data Storage Devices*** 259
- **political beliefs** 5, 91
- **political parties**
  - membership 91
- **polls**
  - collection of personal information 189
- **post-secondary educational bodies**
  - alumni records 214, 236
  - archives 242–45
  - calendars 199, 218
  - class photographs 87, 218
  - common programs or services 225
  - course evaluations 237
  - enrolment information 87, 218
  - governing bodies 12, 131
  - graduations
    - lists of graduates 218, 219
  - heads 23
  - *in camera* meetings, authority for 132
  - peer evaluations 103
  - program eligibility 196
  - teaching and research materials 9
  - teaching evaluations 237
- **power of attorney**
  - exercising rights of individuals 247
- ***Powers of Attorney Act*** 247
- **pricing criteria** 77
- **pricing structures** 74, 148
- prisons and penitentiaries, *see* **correctional authorities or institutions**
- **privacy**
  - audits 264, 302, 371–77
    - FOIP Coordinator 24
  - deceased individuals 86, 217, 235–36
  - harm 82–96
  - not unreasonable invasion of privacy 82–89, 217–19
  - protection 1, 24, 25, 82–96, 187–248, 261–86, 371–77
    - delegation of authority 26
    - information technology and systems 257, 261–86
    - monitoring 289–90
    - offences 29
    - policies and procedures 377
    - public interest 183
    - reports to be published 165
    - request for non-disclosure 88, 217
    - research subjects 84
  - technologies to enhance 262
  - unreasonable invasion 89–96
    - determining 91–95
- **privacy impact assessments** 263–74, 371–77
- **privileged information** 153–63
  - case-by-case privilege 160–61
  - Crown privilege 160
  - Information and Privacy Commissioner 294
  - law enforcement 158
  - legislated privilege 159
  - litigation 156–57
  - parliamentary privilege 159, 344
  - public interest 154
  - severing 60
  - third parties 156–57, 161
    - private records 160
  - waiver of 157–58
- **prizes** 194, 219
- probate, *see* **estates**, administration of
- **probation** 114, 115, 196, 234
- proceedings, *see* **legal proceedings**
- **products**
  - design 74
  - price regulation 77
  - testing 142, 149–50
- **professions**
  - licences and permits 85, 217
- **profit and loss statements** 74
- **programs and services**
  - administrators 25
  - applications for 196
  - attendance 88, 218
  - collection of personal information 190
  - comments by Information and Privacy Commissioner 290
  - common programs 224–25
  - continuing eligibility for 197
  - eligibility 196–97, 201, 226–27, 238
  - evaluation 219, 238
  - expansion 238
  - FOIP contacts 25
  - integrated programs 224–25
  - manuals and guidelines 32–33
  - plans 139
  - policies
    - interpretation 143
  - rules 143
- **programs of study** 102

- **property**
  - assessment information 219, 238
  - *in camera* meetings 132
  - licences and permits 85, 217
  - ownership 219, 238
  - rental values 77
  - security 87, 113
- **Proposal to Access Personal Information for Research or Statistical Purposes Form** 391
- **proprietary interest** 147–48
- **proprietorships**
  - sole 167
- **prosecution records** 10, 111–12
  - 10 years old or more 112
- **prosecutions**
  - appeal period 10
  - decisions not to proceed 116
  - discretion to proceed 111–12
  - protection from 185
  - stays 10
- ***Protection for Persons in Care Act*** .. 99, 158
- Protection of personal privacy, *see* **privacy**, protection
- **Provincial Archives of Alberta**
  - 75-year-old records 244
  - church records 10
  - disclosing business information 80
  - disclosing personal information to 229–30
  - disclosure of personal information 242–45
  - information 25 years old 244
  - labour union records 10
  - policies and procedures 245
  - private records 10
  - records excluded from the *Act* 10
  - transfer of records to 48, 210, 229, 242, 244, 251, 258
  - unrestricted records 4, 242
- **Provincial Court of Alberta**
  - excluded from *FOIP Act* 3
  - records 7
- **provincial governments**
  - intergovernmental relations 119
- **provincial health boards** 2
- **provincial public bodies**
  - defined 2
  - FOIP Coordinator 24
  - heads 23
  - personal information banks 31–32, 273–74
- **psychiatric institutions**
  - patients 113
- **psychiatrists**
  - expert consultations 98, 99, 232
- **psychological tests** 152
- **psychologists**
  - expert consultations 98, 99, 232
- public accountability, *see* **accountability**
- **public bodies**
  - administration 139
  - agreements
    - collection of personal information .. 189
  - assets 146
  - business plans 139
  - competitive position 148
  - consultations or deliberations 138
  - decision-making processes 137–38
  - defined 1
  - discretionary benefits 85–86
  - economic interests 145–51
    - harms test 145–46
  - excluded from *FOIP Act* 3
  - financial gain 77
  - financial liabilities 146
  - financial loss 77
  - harassment 37
  - honours and awards 88, 219
  - investment strategies 146
  - liability 67
  - manuals and guidelines accessing ... 32–33
  - minutes 140
  - negotiations 149
  - officers
    - disclosing personal information to 223–25
  - plans
    - implementation 139
  - preparing for reviews 296
  - programs and services, *see* **programs and services**
  - public scrutiny 92
  - roles and responsibilities 23–27
    - confidential information 75
  - sharing of personal information 193, 265, 278
  - testing for purchase 142, 149–50
  - trade secrets 147
- **public events**
  - attendance or participation 88

Public Guardian 197
public health
  disclosure of personal information . 92–93
  fee waiver 55
  inspections 116
Public Inquiries Act 291, 298
public interest
  case-by-case privilege......................... 160
  data linkage... 240
  determination 182
  disclosure 178–85
    mandatory exceptions......................... 68
    notices 183, 359, 360
  fee waiver 55
  harmful disclosures......................... 76, 77
  not contrary to......................... 86–89, 217
  personal information disclosure..... 86–89, 92–93, 180, 216, 217
  privilege 154
  research benefits 240
  third party consultation 183–84
public interest override................... 178–85
Public Lands Act 222
public meetings............................. 132, 133
public registries, *see* **registries**
public relations.. 25
public safety
  disclosure harmful to 98–101
  disclosure of personal
    information 92–93
  fee waiver 55
  harm to.. 181
public scrutiny
  and privacy 92
Public Service Act 233
Public Trustee 197
publications, *see* **reports and publications**

Q

quality assurance committees 8
quality assurance records................. 8, 228
quasi-judicial tribunals............................. 8
  disclosure of personal information
    to.. 232–33
  draft decisions.. 7
  rules 4
question period 127
questionnaires
  collection of personal information...... 189

R

racial origin.. 91
  personal information 5
RCMP.................................. 4, 106, 230, 231
real property, *see* **property**
recommendations
  officials 137–38
records
  5 years old
    Cabinet decisions............................ 128
  15 years old
    advice from officials....................... 141
    Executive Council or Treasury
      Board 126
    intergovernmental relations 122
    local public body confidences 133
  50 years old
    businesses 80
  75 years old
    personal information....................... 244
  access 31–66
  alumni 214, 236
  annotation 205–7
  available without FOIP request....... 16–18
  banking 13
  businesses 73–74
  classification systems......................... 255
  compelling production 5, 291–92
  confiscated 112–13
  constituency 3, 11, 12
  consultants 6
  contractors............................ 6–7, 47, 259
  copying 48
  correcting 205
  correctional records............................. 114
  counsellors 6
  courts... 7
  creating and generating. 6, 20, 51, 59, 255
  creation for ease of severing 61
  credit unions.. 13
  Crown 160
  custody or control 6–7
  defined 5
  destruction............. 5, 47, 251–53, 258–59
    documentation 63, 251–53
    offences 29, 48, 210, 252
    unauthorized 210–11
  directories of holdings 18, 19, 26, 28, 31–32, 255, 274

  - disposition 5, 6, 47, 48, 251–53, 258–59, 270
    - FOIP requests 65
  - elected officials 11–12
  - examination of 33
    - fees 51
    - Information and Privacy Commissioner 292, 298
  - excluded from *FOIP Act* 7–14, 64
  - Executive Council 124–29
  - failure to locate 63
  - falsification
    - offences 29
  - FOIP requests 62, 65
  - judicial administration 7
  - justices of the peace 7
  - labour unions 10
  - law enforcement 62, 90, 105–18
    - records of disclosure 230
  - line-by-line review 57–59
  - linkage 205–7, 240, 288
  - medical 8, 160
  - ministers 10
  - MLAs 3, 12
  - modifying for routine disclosure 20
  - offences 29, 48
  - Ombudsman 8
  - personal information accuracy and retention 201–3, 269–70
    - audits 373–74
    - correction 203–8
    - disclosure for archival purposes 229–30
    - unauthorized destruction 210–11
  - public events and activities 88, 218
  - refusal to confirm or deny existence 63, 95–96, 343
    - harm to health or safety 65, 99
    - harm to law enforcement 65, 117
    - notices 343
    - personal information 65
  - responsive information 59–60, 61
  - retention 5, 48, 270
    - by Information and Privacy Commissioner 298
    - FOIP requests 65
    - personal information 201–3, 229–30, 269–70, 376–77
  - retrieval 47, 49, 250–51, 255
  - review of holdings 19, 49
  - routine disclosure 14–21, 253
  - scheduling 251–53, 258–59, 270
  - searching 47, 49, 250–51, 255
  - security 25, 26, 256
    - audits 373–74
  - storage 5, 7, 203
    - searching 47, 251
  - third parties 73–74
  - transfer 5
  - transfer to archives 242, 244, 251, 258
  - transitory 48, 202, 211, 252, 256
    - local public bodies 256
  - Treasury Board 124
  - treasury branch 13
- **records management** 25–26, 249–59
  - contracts and contractors 259
  - Information and Privacy Commissioner 250
  - information dissemination 19
  - information technology and systems 256–59
  - local public bodies 5, 249–59
  - personal information banks 376
  - policy and procedures 254–59
  - principles 253–54
  - security 26, 256
  - systems 255
- **Records Management Regulation** 203, 210, 249, 254, 258, 259
- ***Records Scheduling and Disposition in the Government of Alberta*** 211, 249, 256, 258
- **references**
  - character 91
  - employment 91, 102, 198, 221
- **regional health authorities** 2
  - disclosing personal information to 222
  - governing bodies 12
- ***Regional Health Authorities Act*** 2
- **regional services commissions** 2
- **registrars**
  - companies 10
  - corporations 10
  - land titles 10
  - motor vehicles 10
  - vital statistics 10
- **registries**
  - records 10
- **regulations**
  - drafts 139–40
    - Executive Council 126
  - interpretation 143

relatives 193, 218
relevant circumstances
  unreasonable invasion of privacy 91–95
religious beliefs 5, 91
remote areas
  FOIP requests 34
repetitious FOIP requests 36
reports and publications
  arbitration 77
  available for purchase 165
  completed research 141
  disclosure 165–66
  failure to publish 166
  fund-raising 194
  Information Management and Privacy, *see* **Information Management and Privacy**, publications
  inspections 75
  labour relations 77
  law enforcement 116
  routine disclosure 15
representatives
  authorization of 248, 391
  consent to disclosure 83
  exercise of individual rights 17, 246–48
  notices 248
  personal information requests 36, 63
  requesting reviews 296
reputation
  corporate or financial 77
  deceased individuals 94
  personal 95, 240
  public bodies 148, 250
Request Summary Form 391
Request to Access Information Form 391
Request to Correct Personal Information Form 391
research
  agreements 240–42, 391
    security 240
  background 142–43
  benefits to be in public interest 240
  business information 80
  genealogical 86
  grants 102
  historical 86, 149
  incomplete 140–41
  Information and Privacy Commissioner 288
  law enforcement 105
  medical 149
  methodology 143
  not unreasonable invasion of privacy 243
  personal information 84, 232
    agreements 240–42, 391
    disclosure for 238–45
  priority of publication 149
  public body employees 149
  purposes
    personal information 239
  reports and publications 140–41
  scientific 142
  teaching and research materials 9
  technical 142
resolutions
  drafts 130
response times 45
responsive information, *see* **FOIP requests**, responsive information
retention, *see* **personal information**, retention; **records**, retention
retrieval of records, *see* **records**, retrieval
revenue
  FOIP 54
  general revenue fund 54
  generation 146
  licensing databases 20
  loss 77, 148
Revenue Canada 230
  verification of income 221
reviews 1, 295–302
  abandoning requests 57
  adequacy of search 47, 250
  adjudication 42, 302–3
  correction of personal information 205
  disclosure of third party information 172, 173
  documentation required 296
  evidence 38
  failure to disclose in public interest 184
  fee waiver requests 55
  fees 53
  preparing for 296
  privacy of deceased individuals 295
  process 297
  refusing access 68
  requesting 63, 296
    forms 391
  retention of records reviewed 203

- third parties 42
  - decision to disclose information 173
- time extensions 42
- time limits 296, 299

right of access, *see* **access rights**
routine access, *see* **routine disclosure**
routine disclosure 4, 14–21, 25, 37
- creating new records 20
- delegation of authority 19
- historical practices 71
- information technology and systems 257
- inspections 19
- personal information 4, 17–18, 216
- records management 253

Royal Canadian Mounted Police, *see* **RCMP**
royalties 79
rules of court 4

S

sabbaticals, *see* **employment**, educational leave
sabotage 109
safety
- disclosure endangering 83–84, 87
- disclosure harmful to 98–101, 218
- harm to 181
- imminent danger to 236
- inspections 116

Safety Codes Act
- inspections 116
- investigations 106

salaries and benefits 90
- plans 139
- ranges 74, 84, 217
- third parties 74

sanctions, *see* **penalties or sanctions**
scholarships 86, 102, 194, 219
School Act 2, 10, 106, 141, 190
school boards 2, 87
- appeals
  - reasons for decision 141

school trustees 11
schools 90
- class photographs 87, 218
- closure 45
- disclosing personal information 222
- enrolment information 87, 218
- graduations
  - lists of graduates 218, 219
- reunions 87, 218

science fairs 219
scientific information 74, 148
Secretary to Cabinet
- correspondence 126

securities commissions 231
security
- communications systems 113–14, 279
- computers 113–14
- contracts and contractors 280
- defined 106
- electronic data 25
- harm to 113–14
- heads of state meetings 109
- information technology and systems 106, 209, 278–79
- investigations 106, 280
- law enforcement 105
- local public bodies 106
- national 108–9
- penalties and sanctions for breach 280
- personal information 208–11, 270–71
  - audits 373–74
  - research agreements 240
- personnel 279
- physical 209
- policies and procedures 208
- property 87, 113–14
  - *in camera* meetings 132
- records management 25, 26, 256
- sporting events 109
- vehicles 108, 113

security impact assessments 265–66
senior citizens
- personal information 222

senior officers
- disclosure statements 9

senior officials
- advice and deliberations 135

Seniors' Advisory Council 13
sensitive information
- applicant identification 63
- exceptions to right of access 16, 67, 96, 99
- personal information 92
  - proof of identity 63
- security 278

severing information 59–62, 71
- FOIP Coordinator 24

- impracticality 239
  - indicating 61, 339-41
  - Information and Privacy Commissioner 297
  - law enforcement records 62
  - line-by-line review 57–59, 71
  - manuals and guidelines 33
  - non-responsive information 60
  - procedures 59, 61–62
  - refusal of access 61
  - solicitor–client privilege 154
- **sex**
  - personal information 5
- **sheriffs** 113
- shredding, *see* **records**, destruction
- **smart cards** 262, 290
- **smuggling** 111
- **social service benefits** 86, 90, 222
  - continuing eligibility for 197
- **software** 5
  - economic interests of public bodies 147
- **soil tests** 142, 149
- **solicitor–client privilege** 154–56
  - severing 154
- **Speaker of the Legislative Assembly** 289
  - office 3, 12
  - parliamentary privilege 159, 344
  - records excluded from *FOIP Act* 3
- **special areas** 2
- ***Special Areas Act*** 2
- **special constables** 102, 106, 113
- **sporting events**
  - lists of participants 219
  - photographs 219
  - security 109
- **Standing Policy Committees** 13, 124
- **statistical information**
  - law enforcement 116
  - personal information 84, 232, 238–42
  - proprietary interest 148
  - surveys 142
- **statutory holidays** 45
- storage, *see* **records**, storage
- stress, *see* **health**
- **Student Record Regulation** 190
- **student records** 224
- **students**
  - course evaluations 237
  - disclosure not unreasonable invasion of privacy 84
  - emergency contacts 194
  - loans 201
  - timetables 87
- **Subdivision and Development Appeal Boards** 8
- **subpoenas**
  - disclosing personal information 223
- **subsidiary health corporations** 2
- **substance of deliberations** 125
  - Cabinet confidences 125
  - local public body confidences 130–34
- ***Suggested Elements for a Privacy Impact Assessment*** 265
- **suicide** 98, 236
- **Superintendent of Financial Institutions** 230
- supplied in confidence, *see* **confidential information**
- **surveys**
  - collection of personal information 189, 199
- symbols, *see* **numbers or symbols**
- **systematic FOIP requests** 36

T

- **tax information**
  - disclosure 78–79
  - personal information 91
  - rulings
    - routine disclosure 19
- **taxes**
  - arrears 78
  - collecting 79, 146
  - determining liability 78
  - returns 78
- **taxi licences** 85
- **teachers**
  - certificates and permits 85
  - course development 148
- **teaching materials** 9
- **technical information** 74, 147–48
- **technical institutes** 2, 10
- ***Technical Institutes Act*** 2
- telecommunications, *see* **communications systems**
- **telephone**
  - collection of personal information by 200
- **telephone directories** 165, 235
- **telephone numbers**
  - personal information 5

- **temporary absence permits** 114
- **territorial governments**
  - intergovernmental relations 119
- **terrorism** 109
- **testing procedures** 74
- **tests**
  - drugs 142
  - environmental 142, 149–50, 152
  - fee for service 149
  - intelligence 152
  - landfills 142
  - methods and procedures 142, 149–50, 152
  - products 142, 149–50
  - psychological 152
  - questions 9, 152
- **third parties**
  - burden of proof 300
  - competitive position 76
  - confidential information 74–75, 94
  - consent to disclosure 79, 170–71, 221
  - consultations 42, 167–76, 345–61
    - non-response 171
    - public interest 183–84
    - responses 170–71
  - custody of records 6
  - disclosure of information authorized by enactments 79, 84
  - financial gain 77
  - financial loss 77
  - harm to business interests 73–81
  - identities 170
  - information jointly compiled 74
  - labour relations 77
  - negotiating positions 76, 149
  - notices 45, 167–72, 345–61
    - content 169–70
    - personal information 84
    - public interest 183–84
  - personal information 15, 94
    - correction 207–8
  - personnel management 74
  - privacy 82–96
    - not unreasonable invasion 82–89
    - unreasonable invasion 89–96
  - privileged information 156–57, 161
    - private records 160
  - public events 88
  - refusal to supply information 77
  - responses 170–71
  - routine disclosure 15
  - tax information 78
  - time extensions 42, 174–75
  - time limits 172–74
  - trade secrets 73
- **time extensions** 38, 42–45
  - complaints 45
  - documenting 44
  - investigations 301
  - limits on 43, 44
  - notices 45, 331–32
  - third parties 42, 174–75
- **time limits**
  - adjudication and adjudicators 302
  - complaints 302
  - compliance with Information and Privacy Commissioner's orders 300
  - correction of personal information 205, 207
  - FOIP requests 38, 41–46, 49
  - judicial review 303
  - producing records for the Information and Privacy Commissioner 298
  - requesting reviews 296
  - reviews 299
  - third parties 172–74
  - transfers 40
- tracking systems, *see* **FOIP requests**, tracking
- **trade**
  - associated states 109
  - deals 146
- **trade secrets**
  - ownership 74, 147
  - public bodies 147
  - third parties 73
- **training** 24, 28
  - personal information 90
    - security 208
  - routine disclosure 20
- **transfers**
  - FOIP requests 39–41, 45, 49
    - notices 330
  - personal information requests 39–41
    - correction of information 208
- **transitory records** 202, 211, 252, 256
  - disposition 48
- **Transmittal Memorandum (Sample)** 391
- **travel claims**
  - routine disclosure 19

Treasury Board
  - agenda 125
  - background facts 127–28
  - decisions 127–28
  - minutes 125
  - non-arm's length transactions 13
  - records 124

treasury branches, *see* **Alberta Treasury Branch**

Treasury Department, *see* **Alberta Treasury**

treaties 109
  - aboriginal people 120
  - disclosing personal information 221
  - law enforcement 231

trespass 106

tribunals 112

trustees 95
  - exercising rights of individuals 247

U

unemployment insurance, *see* **employment insurance**

UNESCO 120

United Nations 120

United States Immigration and Naturalization Service 231

universities 2, 10, 90
  - enrolment 87
  - reunions 87, 218

Universities Act 2

use of personal information, *see* **personal information**, use

V

vehicles
  - accidents 236
  - security 108, 113

vexatious FOIP requests, *see* **frivolous or vexatious FOIP requests**

video tapes 194, 209

visually impaired persons
  - FOIP requests 34

Vital Statistics Act 10

voice mail 256

volunteers
  - disclosure not unreasonable invasion of privacy 84, 217
  - disclosure of personal information to 223–25

vouchers 5

W

waivers, *see* **fees**, waivers

wardens 113

warrants
  - disclosing personal information 223

weapons
  - technical information 113

welfare, *see* **social service benefits**

whistle-blowing 184–85, 291

wire-taps 109, 115

witnesses
  - compelling attendance 5, 291, 298
  - protection 98
  - statements 190

Workers' Compensation Act 192

work-experience programs
  - personal information 84, 225

Y

Young Offenders Act 113

***Young Offenders Act* (Canada)** 115